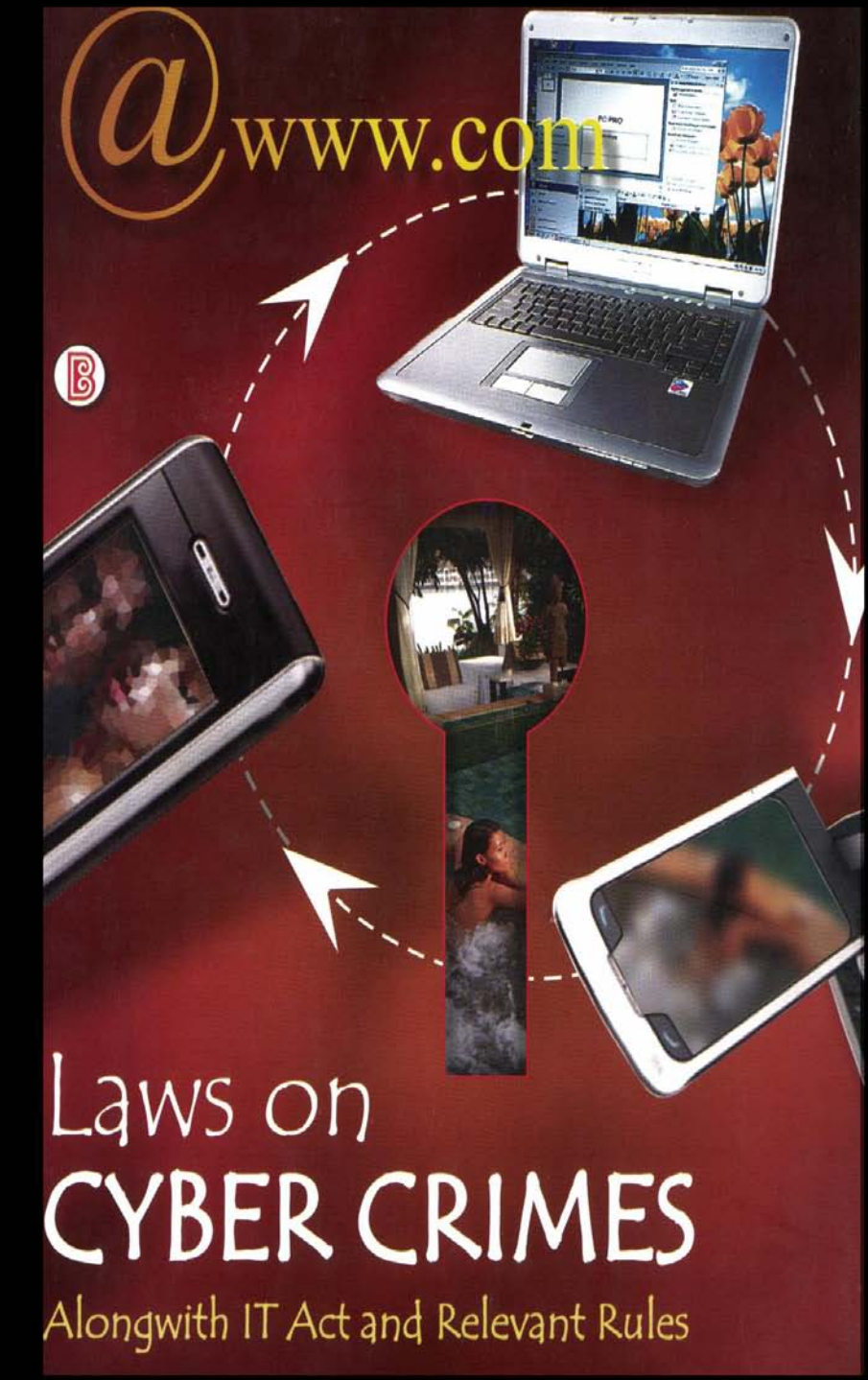

Laws on CYBER CRIMES

Alongwith IT Act and Relevant Rules

Laws on Cyber Crimes

[Alongwith IT Act and Relevant Rules]

Dr. Pramod Kr. Singh

Book Enclave
Jaipur India

Note: (1) No part of this book can be reproduced or copied in any form.

(2) All possible care has been taken while preparing and publishing this book and the author, publisher and printer shall not be responsible at all for any kind of error or omission found, if any, in this book. Readers must cross-check from original Government notification and other materials.

ISBN : 978-81-8152-163-7

First Published : 2007

ISBN : 81-8152-163-3

© Reserved

Published by

Book Enclave

Jain Bhawan, Opp. N.E.I., Shanti Nagar, Jaipur - 302006 Tel. 0141-2221456

Showroom

G-13, S.S. Tower, Dhamani Street, Chaura Rasta, Jaipur

Tel. 0141-2311900, Fax: +91-141-2311900, E-mail: bookenclave@yahoo.com

Laser Typesetting by

Pushpendra Shekhawat, Jaipur

Printed at

Roshan Offset Printers, Delhi

Contents

"This page is Intentionally Left Blank"

Part-I

"This page is Intentionally Left Blank"

1

Information Technology and Cyber Crimes : An Introduction

Synopsis

1.1. Information Technology : An Introductory note

Crime is not a single phenomenon that can be examined, analysed and described in one piece. It occurs in every part of the country and in every stratum of society. The offenders and its victims are people of all ages, income and backgrounds. Its trend

are difficult to ascertain. Its causes are legion. Its cures are speculative and controversial. Computer related crimes, popularly called as Cyber Crimes, are most latest among all the crimes.

- *Cyber Space*

William Gibson in the science fiction ("Neuromancer") coined the word "Cyber space" in 1984. Basically it denotes the virtual location within which electronic activities takes place. Cyber space is a borderless environment. It has no territorial based boundaries. The internet address has no relation to the physical location of computers and individuals accessing them thus render geographical borders of nations meaningless. The geographical boundaries of nations and the electronic frontiers do not have any co-relationship. Since nations assert authority or the basis of territorial nexus over individual, events and happenings occurring within its jurisdiction, when territorial borders lose their meaning, well settled principle of international law is threatened. Cyber space, thus, challenges the well-established principle of international law that control over physical space and people is an attribute of sovereign and statehood.

- *IT Evolution in India*

Information Technology is one of the fastest growing technologies in the world. Rapid transformations are taking place from a system of control for liberalisation and globalisation of information technology. The information is being recognised as a source for the development of countries. Government of India has taken various initiatives and measures for introducing appropriate automation to increase productivity and for the production of quality products and services. The availability of trained personnel is a plus factor. The timely availability of accurate, reliable and consistent information on various accounts is an essential factor for the government, corporate or industrial sectors. Indian organisations are gearing up to meet the challenge of managing the changed environment. For this, system and technology have to integrate with the organisation to provide qualitative information available at appropriate levels and appropriate time for decision-making. Information technology plays a major role in this through collection, organisation, storage and dissemination of information not only at the place of origin but also at various other appropriate locations by using

appropriate communication infrastructure. The Internet, in simple terminology, means an international networks of computers of various types ragging from notebook computers to show computers connecting 2 million computers of 13,300 networks providing service to over 50 million users worldwide. This is also known as the 'World Wide Web' or information superhighway. Each individual network within the internet is also called a 'Website'.

- ***Common Cyber Crimes***

Hacking, cracking, sending obscene e-mail, tampering of source codes, e-mail abuse, e-mail spoofing, e-mail threat, sending obscene SMS, post defamatory profile on net, mishandling of copy right acts, cyber stalking, identity drift, phreaking, carding, etc., are the crime most likely in the world.

Cracking : A person can delete files or put a virus up or sell information or steal some source codes and could use it for his own benefit. He can also perform a denial of service attack and cause the computer to stop working.

E-mail Spoofing : A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. E-mail spoofing can also cause monetary damages.

Cyber Stalking : It involves repeated threats and harassment of a victim through e-mail, chat message or web pages.

Phreaking : Covers a wide variety of activities concerning the abuse of the telephone networks.

Carding : The term can be used for involving the illegal use of any type of credit case.

1.2. Cyber Crimes : Glimpses

The cyber crimes may be of various types affecting privacy, person, state, prestige, property, nation etc. at different levels. These are some of the burgeoning incidents of cyber crimes in our country :

- A Delhi based girl, Ritu Kohli, becomes the victim of first ever case of cyber stalking reported in India. The accused was booked under the relatively innocuous section 509 of the Indian Penal Code.[1] The accused is abroad based.
- A Delhi school boy photographed a fellow girl student with his camera cell phone and then sent the pictures as an MMS to other students.[2]

- Two class XI students of Delhi Public School, R.K. Puram, New Delhi land in controversy regarding sexually explicit MMS.[3]
- In January 2004, 28 year-old software engineer was arrested for hacking a woman's e-mail password and sending obscene message through the same account to her office colleagues after she refused to marry him.[4]
- A man threatened to put up morphic pictures of an employee of an embassy in New Delhi on sex portals on her refusal to pose in nude for him.[5]
- In August 2004, an airline employee sent morphic pictures of his boss' wife to his colleagues for the reason that he was apparently upset with his boss for not treating him well.[6]
- An employee of the Bank of India was caught tapping his own organisations network and he gathered data including passwords by way of monitoring the ECTV.[7]
- An MBA, Akash Singh hacked in an ATM centre with the help of counterfeit card to withdraw several lakhs of cash from Canara Bank of Chennai branch.[8]
- A Canadian hacker on 7 February, 2000 broke into the Yahoo's system and disturbed whole system.

1.3. Cyber Crimes : Definition and Scope

Cyber crime, in a general sense, is an act that covers the entire range of crimes which involves computer, computer network, cell phones, etc., either as its target or as an instrumentality or associate. Thus any kind of criminal activity that takes place with the help of or against such electronic equipments and in the cyber space, comes under the purview of the word cyber crimes. Like other criminal activities, the motive or intention to cause an injury is one of the ingredient and the same is not limited to any specific type. The criminal conduct in the cyber world begins from the activity of stealing computer hardware and ends to the extent of transferring, altering or damaging, the computer data to cause harms to Net users.

A lady in U.K. received a package of perfume she often used at her home through the internet stopping, though she had not

placed any order for the same. She again got the next package and this continued till she received 25 more packages. Soon she discovered that someone had stolen her credit card details and was playing prank on her by way of ordering perfumes and such other things for her. But she could detect and take remedial measure, much damage has already been occurred to her. After sometime, the bank refunded the lady's money and wrote a latter to the online shopping to gather information about the cracker. She approached police also with information collected by police but nothing could be done.

The above incident is an example of what we cell the "spoofing". According to the Internet Protocol (IP), the "Spoofing" is a method of making you to face a situation when you feel that you are connected to internet in the location, when you could really be anywhere else on the planet. Sometime the crackers' activities of cracking are much damaging. Some crackers are found working for organised gang of criminals. Such crackers, sometimes transfer money from by intervening into the internet banking accounts. Usually the crackers are big business houses and their IT systems that range from simple defacing a site to the extent of stealing a database of credit card numbers or other sensitive company information. The incidents of such types of cyber crimes are increasing. According to information available, about 225 incidents were reported in 2002 in U.K., which rose up to 1000 in September 2003.

"Spamming" involves sending of bulk and repeated unsolicited e-mail to any person. In other words, we can say that spamming is an act which involves bulk, mass or repeated posting or mailing of substantially identical messages. Mr. Howard Carmack was a notorious cracker, who used to send out millions of e-mails that included advertisements for computer virus scripts, work-at-home scheme, be rich quickly and also the list of addresses to be used by other spammers.

Macomb Area Computer Enforcement Team (MACE) is a task force of law enforcers in U.S.A. who deal with computer related cyber crime. MACE has arrested an Indian student named as Ram Chandran Karthikeyan, aged about 25 years, at somewhere in Harrison township of Michigan state. He was arrested when he was supposed to meet a 15-year old girl who he used to entice

through internet for sexual intercourse. This task force has arrested about a dozen suspected child predators since 2001.

A youngman in U.K. was sentenced for two years in jail by a court in Steinbach, Manitoba, for cyber stalking a Candian woman. Christopher Kell, 37, a native of Cumbria, was arrested for sending thousands of "harassing e-mails, letters, and faxes, who he had met in an internet chat room. They had later met at Paris but their relation soon ended when Kell started sending her absurd e-mails. He also sent nude photographs of women to her family and local business houses.

An employee working with an embassy in New Delhi, Seema, could never imagine that Web Surfing could lead to the invasion of her privacy to such extent. Seema, in the wake of cyber stalking, received a series of e-mails from a man asking her to either pose in the nude for him or to pay Rs. one lakh to him. The cracker threatened her that he would display her morphed picture at sex websites, along with her telephone numbers and address. The man also threatened to put her pictures in her neighbourhood in the South West Delhi. The hacker went to the extent of mailing her photographs, which she claimed to keep in her mail folder. According to Delhi Police, the accused had successfully hacked her e-mail password and there- by could access to the pictures. The preliminary enquiry revealed that the e-mail were sent to the victim from a cyber cafe in South Delhi.

The episode of "Love Bug" virus had created have all around the world. The virus appeared in "Hong Kong on May 11, 2000 and spread rapidly through the world. The virus destroyed thousands of files and stole password almost all around the world. In Hamburg, the virus ruined about 2000 digital photograph in the picture gallery and diabled ATMs centres the Belgium leaving lakhs of people cashess. The virus affected NASA and CIA also for nearly two hours.[9] According to estimate available, the estimated damage was ranging from two billion dollars up to ten billion. This incident reflected on the inherent difficulty of assessing the harm inflicted by cyber crime.

Virus experts soon traced the Philippines as the place of origin of the "Love Bug". Although the agents of FBI and National Bureau of Investigation could identify the persons suspected of creating and disseminating the "Love Bug" using information

supplied by the internet server but they landed into problems with the investigation. The authorities faced difficulty in taking legal action against the cyber criminals since the Philippines had no cyber crime laws. The act of creating and disseminating the virus was not a crime in the country in absence of specific law. Since the act was no crime, the investigating agency faced much difficulties convincing a magistrate to issue a search warrant agency faced much difficulties convincing a magistrate to issue a search warrant to enter into the suspect's appartment. After finally executing the warrant and seizing the evidences, they could found that Onel de Guzman, a former computer science student, was responsible for creating and disseminating the deadly virus, the "Love Bug". As hacking and the distribution of damaging virus had not been a criminal act there, the officials could book him only for theft and fraud of credit card. In absence of a proper extradition treaty, Guzman could not be extradited for prosecution by other countries where there were cyber laws', such as the U.S.A. Despite having caused damages to the tune of billions of dollars all around the world, Guzman could not be prosecuted and brought to the trial in the matter. This incident realised the necessity of promulgation of a cyber law in every country of the world. Thus, no one could be prospected for the damage caused by the "Love Bug".

1.4. Nature and Extent of Cyber Crimes

We could see above some glimpses of what we call the cyber crimes. Cyber crime in usual term may be called a criminal act that covers the entire range of crimes occurring with computers or computer networks and cell phone, etc., either as its target or an instrument for such act. Any kind of criminal activity occurring in the place called cyber space and resulting any loss or damage of instrument, data, information, knowledge, privacy, etc., comes under the purview of cyber crimes. Like other criminal activities, the cyber criminality is not limited to any specific type. The conduct in cyberspace may vary from the minor activity of invading privacy by sending obscene MMS to the extent of stealing secret and sensitive information stored in the memory of a person or firm or state.

The impact of cyber crime is not limited to any particular region or any particular target group. Any internet user may

become the victim of cyber crimes. In the today's fast increasing world of Information Technology, nobody can remain immune from the impact of cyber crimes. When entire human activities are now dependent upon the information technology and computer based infrastructure, all these activities are naturally vulnerable to the cyber crimes. Entire human activities, such as Banking transaction, Defence equipments, Online trade, Stock exchange transactions, Education a laboratories, Personal datas (financial, medical, confidential, etc.), etc., are now fully dependent on the cyber equipments. The users list is so large and unending that no demographic profile of potential victims can be prepared. The victims of cyber crimes are not limited to those who are computer users but it may affect anyone living anywhere in the world. For example, if a computer hacker changes the medical prescription stored in the memory of hospital's computer, the patient undergoing treatment may be affected severely.

1.5. Cyber Crimes : Know no Boundaries

The cyber crime is unique among all types of crimes in the sense, *inter alia*, that it knows no distance, boundary and time. Usually in a crime the offence is committed at a particular place and the offender belongs to the same place. Since the place of occurrence (PO) is at the same place, it is rather simple to deal with such type of crimes. But in case of a cyber crime the offender at U.S.A. may commit a crime against a victim in India. So there are many hurdles right from the stage of lodging of FIR to making a successful investigation. In other words, we can say that in the world of present day's information technology and cyber space, person sitting in a nearby room and persons in the fathest country are quite equal in terms of distance. For even comparatively a minor crime committed in one of the small town of India through a computer network or cell phone, the process of investigation might extend to the whole country or the whole world.

Cyber space is not confined to any territional boundaries because the cost, time and speed of message transmitted through the internet is completely free from any physical location. Message can be transmitted from are part of the world to the another part of the world within seconds. Such transmission is quick without any kind of degradation, decay or substantial delay. The internet enable exchange of message between parties, who do not know

the physical location to each other. The knowledge of ocation between both parties is simply the "web addresses" or "websites" of computer sets. The system is quite indifferent to the physical location of these computer sets and there is no need of necessary connection between an internet address and a physical location.

1.6. Rapid Transmission and Accuracy

The invention of internet has come up as a boon both to common folk and criminals. The unlimited utility of internet and cell phones has the criminals towards cyber world. They has opted the new methods of information technology to commit traditional forms of crime in more sophisticated, accurate and faster ways. The large scale use of internet message by the criminals attacking Indian Parliament may be taken as the appropriate example. Major criminals and terrorists organisations are not funding themselves and transmitting plans worldwide through the Net. The ability of making accurate copies through digital technologies is creating serious problems to law enforcing agencies worldwide, in the form of fake currencies, judicial stamps scandal, seizure of large scale fake stamps and foreign and Indian currencies, etc., shown the magnitude of the problem.

1.7. Diversity and Span of Victimisation

Cyber crimes affects every walk of society and it does not discriminate between people of different society and country. An individual submitting her personal details for government agencies or private employer, may find his resume being misused by international criminals. Children visiting chat room may fall prey to the paedophiles prawling. An innocent woman may fall victim to a maniac cracker through e-mails or MMS by of way her identity stolen from a website. A Bank may fall victim of large scale transfer of money through computer fraud committed by one of his employees or somebody else having their access to its computers. A corporate body may be blackmailed by a computer hacker, who threatens to transfer confidential information to their competitor or unscrupulous elements or to make it public, unless they pay him huge money. Thus, the list of potential victims of cyber crimes is virtually endless. The computers of home users may become an easy prey to the hacking activity controlled through distant machines which are often used to allook critical infrastructures. The home users and business computers often

using digital subscriber line (DSH) or cable connections are vulnerable to such attackers who are able to enter into their confidential datas with the knowledge of owners. Large government and non-government agencies, such as corporation, government departments, colleges, universities, etc., are common target of cyber criminals. Such enterprises require adequate security for protection of their information and security policies.

Various organisations working in the sector of the economy, government or academy can reduce the risk of hacking of valuable information by way of sharing such information. Several sectors now have formed Information Sharing and Analysis Centres (ISACs) to monitor the cyber attacks directed against their respective infrastructures. Sometimes cyber security problems have national implications and it cannot be solved by individual enterprises or infrastructure sector alone. The international coordinations are essential for research and development of improved and more advanced technologies.

The world wide web is an internationally shared platform and hence the internationally shared standards enable interoperability among the world's computer network. The international cooperation is essential to share informations concerning cyber crimes and further to prosecute cyber offenders. Without such international cooperation and collaboration, our collective efforts to detect, deter and check the cyber crimes at world level is not possible at all. A hacker sitting in London and intervening the computer privacy at Delhi can be booked only through international coordinations.

1.8. Cyber World : Laws Lags behind Technology

With all marvels of Information Technology (IT), a reasonable apprehension about abuse of the technology has followed the rapid growth of net service. The recent controversy over an obscene MMS clip and its circulation through the internet is apparently worring mobile handset makers. They are worried about a possible black lash against camera phones and the impact it might have on their sales if moves to restrict their abuse does not yield positive results.

Sale of camera phones are rising worldwide including in India, as cell phones have become powerful device of communication that can send byte-heavy pictures and video clip

within a moment anywhere around the world. Cellphones are going much beyond being just talking tools. Unlike the internet, when it is possible up to some extent to block objectionable contents, no such technology exists for mobile phones. Mr. Pankaj Mohindroo, President of Indian Cellular Association (ICA), an industry body comprising the world's leading handset makers, comments, "It's game to take up the responsibility. It is a good idea. Any move by corporates and industry bodies aimed at improving the *tehzeeb* (etiquette) and *tameez* (manners) of consumers and citizens is welcome."[10] Commenting on the abuse of cellphones, Kunal Ahooja, an official of Samsung, which claims to be the first company in the world to issue guidelines for responsible use of camera phones, says, "There is a need to use technology responsibly. Not doing anything about it is even worse. At least we want to caution consumers against inappropriate use of camera phones."[11]

The irresponsible and criminal abuse of mobile phones is a matter of growing concern in schools and colleges. The recent incident where a Delhi School student circulated a mobile video clip of two co-students having sex initiated a heated discussion on whether cellphones needed to be banned in educational institutions. The management of several colleges are schools and saying that it is now time to discourage students from carrying mobiles to college and school campus. Their biggest fear, as they say, is Information Technology (IT) and computer science students who are constantly making new discoveries on their cellphones. Many schools and colleges have already begun banning mobile phones on their premises.

Following the MMS incident, the Principal of Delhi Public School (DPS), Shayama Chona, went ahead and sent a letter to the parents of students in the school mentioning the "moral vacuum" students are facing nowadays. She laments the "existing malaise of rowdyism and behaviours, disrespect to elders, the lack of etiquette and values in general." It attributes the "moral vacuum" to the influences of the television, media, internet and peer group pressures and exhorts parents to empower students through aesthetic, intellectual and cultural refinement.

Worried schools' management have also issued a list 'dos' and 'don't, which includes not to bring cellphones to school,

along with other activities such as sloganeering, signature campaign, wearing shabby and sloppy dresses, bunking classes, wearing garments with slogans on them and so on. However, while schools and colleges try to curtail the mobile menace, the mobile market is doing its best efforts to entice students. A service provider recently introduced 15 campus zones in the city for students who can make calls at two paise per second within a campus zone and three paise per second outside it. SMS for students billed at 50 paise with other freebies such as unlimited SMS to the 'buddy number'. Experts, however, justify the banning of mobile phones in the campus as the abuse of cellphone for fun is now a criminal act under the provisions of Information Technology Act, 2000.

1.9. Inadequacy of Law

The heated debates have been started on the point of success rate of Information Technology Act, 2000. The acts of stalking, harassment, defamation or morphing are emerging and growing fast as a potent manifestation of cyber crime not only in the cities but in the whole country. The law is supposed to deal with the cyber crimes, but the fact is that it is an Act which is mainly prompting legal transactions for e-commerce.

The Chapter XI of the Act entitled 'Of Offences', deals with hacking, damage to computer source code, publishing of obscence information and breach of protected system. It, however, does not cover the act of cyber stalking, mobile phone cloning, and other forms of harassment. An example that can be cited here is that of Delhi-based Ritu Kohli, the victim in the first ever case of cyber stalking reported in India. The accused of the case was booked under relatively innocuous section of 509 of the India Penal Code which is a penal provision for outaging the modesty of a woman. The Act is further inadequate in the sense that it also does not give the police any power or jurisdiction to crack down on websites whose servers are based abroad. The failure of the law in keeping pace with the technology was obvious in the MMS case in which the CEO of Bazee.com was arrested.

A well-known expert of cyber crimes says, "Internet is like huge ocean, and the Act wrongly makes the service provider liable for all third-party data and information posted on it as in

the Bazee case."[12] The act provides that in two circumstances the service provider will not be held accountable, i.e., if he had no knowledge about the displayed information, and if he could not prevent it despite "due diligence" on his part. In both situations, however, the service provider would be presumed guilty, and the onus will be on him to prove himself innocent. The another provision of the Act that only an officer of Assistant Commissioner of Police (ACP) can register or investigate cyber crime cases is also creating a lot of problems and constraints because the number of ACPs are limited as compared with the increasing number of cyber crimes. It is, thus, important to amend the Act but there is also a need for legislation on cyber crimes to supplement the Indian Penal Code (IPC).

It is also imperative on the investigating and enforcement agencies to familiarise themselves with the latest cyber crime investigation techniques, seizure of computer data and its correct presentation in the courts. Otherwise, they will fail miserably before the court in proving the guilt of accused person as it happened with the case of Mumbai Police on an earlier occasion this year when they seized the computer's monitor only, and not the CPV, thinking it to be the "real" computer in a cyber crime case.

1.10. Influence on Teenagers : Views and Counter-views

The adverse effect caused by the abuse of information technological equipments on the adolescents' mind is a matter of growing concern for the parents and teachers. Recent incident in which a Delhi school boy photographed a fellow girl student with his camera cellphone and then sent the pictures as an MMS to other students has aroused a national debate as to whether the children's parents are wrong in giving their son a camera phone ? Whether the student taught the lessons of legal repercussions caused by the abuse of camera cellphone or computer equipments ? Experts say that there are missing or shadowy parents and social pressures on kids in much earlier than in previous generations. The peer relationships, as they believe, account for a great deal of a young person's social and leisure activities. The need to please and be accepted by the peer group than becomes the driving force in teenager's life. Perhaps the Delhi boy was trying to fit into his peer group, but in a misguided way.

The studies show that almost all teenagers consistently give into a peer pressure. A U.S. survey found that many boys feel the pressure to engage in sexual activities even before they are ready. This happens despite the fact that 63 per cent believed waiting for while was a good idea. Another study found that peer pressure is the main reason for girls drinking alcohol. Academic success too is more dependent on peer pressure than family background. This study also noted that even if a child belonged to a less academically inclined family but was part of a peer group which has great emphasis on education, he or she was likely to perform well. Even food habits are largely governed by the tasters of the peer group, according to a U.K. based survey. Therefore, it is the peer group which must be addressed to prevent aberrant behaviours by teenagers. In fact, parents have only a limited role to play.

Other experts blame parents for such incidents. Any parents, as they say, who think it's all right to give a teenager a camera cellphone cannot be absolved of responsibility for such consequences. Children are impressionable and impulsive. It's the parents duty to guide them on to the right path. But parents with too much money and very little time often shower children with goodies to compensate for the lack of attention. With no parental guidance and enough money to splurge, children can easily go to astray.

But the parents have own view to expenses and they show helplessness against their children's pester-power and peer pressure. When a child demands a bigger car because his friends have, he should be firmly refused. But most of new-age parents omit to do it with any conviction. Parents tend to assuage their own guilt by buying their children whatever they want. Good parenting, experts believe, shapes the character of the future adult and no amount of peer pressure can undermine this. Parents are the first teacher and early childhood experiences have a lot to do with moulding a child's personality. Parents are the best role models. Being a good and ideal parent is not an easy job. It needs sweat and blood. But investing time and effort in children is well worth it. When children go astray, it is not good enough to blame the peer group or technologies as the buck stops with parents.

References

1. *The Times of India*, December 30, 2004.
2. *Ibid.*, November 27, 2004.
3. *Ibid.*
4. *Ibid.*, December 20, 2004.
5. *Ibid.*
6. *Ibid.*
7. *Times New Network*, 12 November, 2003.
8. *Ibid.*
9. http ://www.lawtechjournal.com/articles/2002.
10. *The Times of India*, December 12, 04.
11. *Ibid.*
12. *The Times of India*, December 30, 2004.

2

Information Technology : Definition, Dimensions and Influence on Lives

Synopsis

2.1. *Information Technology : Definition and Perspectives*
2.2. *Information Technology : Growth and Future*
2.3. *Information Technology : Various Facets & Dimensions*

- *Computers and its Networking*
- *Cyber or Internet Networks*
  (a) World Wide Web (www)
  (b) Internet Protocol
  (c) Domain Names
  (d) Internet Service Provider (ISP)
  (e) Web Portal
  (f) Search Engines
- *Internet Services*
  (a) Electronic Mail (e-mail)
  (b) Electronic Business (e-business)
  (c) New Groups
  (d) Bulletin Board Service
  (e) Internet Chat
  (f) Instant Messenger

- *Electronic Data Interchange (EDI)*
- *Networking*
  (a) Intranet and Extranet
  (b) Local Area Network (LAN)
  (c) Wide Area Network (WAN)
- *Technology Convergence*

2.1. Information Technology : Definition and Perspectives

The application of information technology is now so wide that there can be none who is untouched by it. The two technology advancements, i.e., computer and the network, have changed the traditional way of human lives. The advanced field of information technology (IT) has now covered every walk of human activities, i.e., manufacturing, marketing, banking, agriculture, communication, airways, education, entertainment, medical, administration of justice, etc. The advent of Home PC, internet and cellphone network have provided us tremendous useful services which have virtually reduced the distance of the world communicable within seconds.

The term IT is, in all-pervasion term, so complex that it is difficult to define what exactly the information technology is. The term IT, broadly speaking, indicates almost all the aspects of managing and processing of information and communication. The IT may be defined as "the devices and techniques used to store, process, manage, transmit and communicate information; encompasses various technologies such as computing, microelectronics and telecommunications.[1] The most important instrument used in the IT is the computer which consists of at least a processor, memory and parts for input and outputs. According to Chambers Twentieth Century Dictionary, the word computer means", a machine or apparatus, mechanical or electric or electronic, for carrying out, especially complex, calculations, dealing with numerical data or with stored items of other information; also used for controlling manufacturing processes, or coordinating large part of organisation.[2] 'Output' is the result of computer processing which could, for example, be presented on VDU display or on a printer. The term 'Input' is the information entered into a computer system for processing or actual entering of data. A personal computer (PC) is a microcomputer whose

main function is for personal use rather than for corporate problem solving.

2.2. Information Technology : Growth and Future

The Information Technology (IT) is although newest yet fastest growing scientific and technological development of the world. It has provided enormous opportunities for the underprivileged countries of the world and opened up new windows for developing countries towards developed countries for transfer of useful knowledges and scientific discoveries. It has happened for the first time in the history of mankind that the technology is not under the control of a particular country or small group of persons. The information has emerged as a new form of power in the present modern information age. The present internet and cyber space services have empowered human being the capabilities of permitting free flow of information beyond all manmade geographical boundaries.

The cyber technology provides equal opportunities for all without differentiating between human beings in the name of sex, caste, creed, race, gender, nationality, etc. In other sense, it has brought a sociological revolution in all the spheres of society and encompasses entire activities of human lives. The tedious calculations, multiple scientific puzzles and industrial puzzles and industrial problems are no longer insurmountable hurdles and the computer has become a hand made of science and industry. A computer is the latest form of service which can accept data, apply a series of logical process to it and supply the results of these processes as information.

The advent of computer has made easier the solution of the complicated problems in technology. All the advanced countries are now taking help of computers in various fields of economic activities. Computerisation in factories and offices results in a great reduction of costs and administrative expenses. The work previously performed by a number of persons can not be entrusted to a computer. By introducing computers, mankind is now able to save a lot. But the disadvantage is that it might create and perpetuate the problem of unemployment. The leaders of trade unions are of opinion that in a country like India where millions of educated youth are suffering the pang of joblessness, it is better we hasten slowly on the road to computerisation.

India has tremendous potentialities for the growth of IT sector. The online shopping market in India has registered 120% increase in revenue within one year and it has grown from Rs. 59 crore to Rs. 129 crore in the year ago period. This massive shift to virtual shopping clearly displays that more and more shoppers are not depending on cyber space and gaining confidence and trust in the online medium. Payment options like cash on delivery and internet banking is becoming popular, encouraging consumers to purchase more. The cellphone market in country is also expected to grow by more than 200% over the next few years as mobile phone usage is expanding fast and subscribers becoming more familiar with the products and services on offer. The Indian market is estimated to grow from $ 26 million in 2004 to $ 3.36 billion of annual revenue by 2009.[3] There can be no denying of the fact that cyber crimes are also most likely to grow in its proportion. Slowly but surely the technology is showing up its ugly face too.

Information Technology : Various Facets and Dimensions

Before one could learn about cyber crimes it is essential that he should know about the basic of computer system and networks. The law relating to the information technology, like other forms of law, are inter-disciplinary in nature. The following are the basis and relevant aspects of information technology.

- ***Computers and Network System***

A computer consists of two major components, i.e., hardware and software. Hardware comprises the physical structure such as Central Processing Unit (CPU), Data Storage Units (Hard disc), input devices like key board, scanner, etc., output devices such as monitors, printers, modems, floppy drives, speakers, web cameras etc. Software is different from hardware. If the hardware is the brain, then software can be termed as mind. Entire knowledge and information is stored in the software and its input and output is done with the help of hardware.

The information which is stored electronically is called 'software'. Software can further be divided into two types, i.e., the program and the data. Program is a series of inter-related instructions capable of performing or achieving a particular task when incorporated into a machine-readable medium. Programme can be expressed in a permanent form, i.e., Read Only Memory

(ROM), or in a transient form, i.e., Random Access Memory (RAM) and the capacitors require periodic charging or refreshing. Programs are usually expressed in a machine-readable language. Software is also divided into two categories, viz., system software and application software. 'System software' includes the operating system and the utilities concerned that enable the computer to function. 'Application software' includes the programs which actually work for users, e.g., word processor, spread sheets and data base system.

The word 'Networking' means an act of establishing interconnection among more than are computers for enabling them to exchange data between them. Networking involves intercommunications between the computers either through physical cables or through communication system including satellites. Network may be a Local Area Network (LAN) which works within a small geographical area like a building or apartment through cable connections, or it can be a Wide Area Network (WAN) connecting computers situated at geographical distances through the medium of communication system such as telephone, satellites, etc.

- *Internet or Cyber system*

'Internet' is the interconnection between millions of computers located all around the world. In other words, internet is a network of networks, local computer system hooked to regional system hooked to national or international high-capacity 'backbone' systems.[4] Each of these connected with each other are managed independently by persons who have opted to adhere to to common communication standards, i.e., TPP/ IP, which makes it possible and practical for adhering to communication. TCP stands for 'Transmission Control Protocol' and IP stands for 'Internet Protocol' and there are the fundamental communication standard.

The network of Internet functions as a pocket switching network in which the information to be transmitted is broken into small pockets of bit that can be transmitted as capacity of the particular connection allows. These packets are levelled with the address of their final destination and follow any number of different routes from computer to computers before it reaches the final destination where the same is again reassembled into the originally transmitted information.

The internet uses the 'smart communications' while transmitting the information. Computers at nod monitor travel on the network independently and route packets along the least congested route to the next node. Such process is repeated until the packet arrives its destination computer. Each computer acts independently and coordinates traffic with its nearest neighbours only. The internet protocol provides for geographically extended sharing of scattered resources. An internet user can employ her internet link to access computers, communicate information or control various types of apparatus all around the world.

(a) World Wide Web (www) : The terms 'internet' and 'World Wide Web' (www) and interchangeable mutually but in fact are two different terms. The web is one of the ways in which information can be disseminated over the internet. The 'Web' is just a portion of internet and an information sharing model built on the top of internet. The web uses http protocol, which is one of the languages used to transmit data. The web also uses browsers, i.e., internet explorer or Netscape, to access web documents called web pages that are linked to each other via hyperlinks. Such web documents also contain graphics, sounds, text and videos. These documents are brought into a script called HTML (Hypertext Markup Language) that supports link to other documents including graphics, audio and video files. The internet user can shift from one document to another simply by clicking on hot spots. Apart from World Wide Web (www), there are another internet servers called Netscape Navigator and Microsoft's Internet Explorer.

(b) Internet Protocol (IP) : Internet is a network of large number of computers consisting of distinct languages and programs. Internet Protocol (IP) is a common language or system which facilitate intercommunication between these computers. It may be called an agreed-format for transmitting data between two computers. The protocol determines some functions, such as the type of error checking, data compression method, sending device transmitting a message and receiving device receiving a message. There are many standard protocols with their own advantages and disadvantages. For instance, some are simpler than others, some are more reliable, and some are faster. The computer must support the right protocol for the sake of communication. The

protocol can be implemented either in hardware or in software. The most common Internet protocols are called HTML, TCP/IP and XML.[5]

(c) Domain Names : The word 'Domain' may be defined as a group of computers and devices on network that are administered as a unit with common rules and procedures. Domain are shown by the IP address in the internet. The said IP address is a string of number such as 222, 243,44, 56, etc. Various devices sharing a common part of IP address are said to be in the same domain.

It is necessary to acquire a domain name in order to operate in the internet. According to an agreement with ICAAN (Internet Corporation for Assigned Names and Numbers), the Network Solutions Inc (NSI) has the responsibility of maintaining a registry of generic top level domain names.[6] NSI is a non-profit organisation functioning under the Department of Commerce of U.S.A. Domain names are of two types, viz., Generic Top Level Domain Names (gTLDs) and Country Code Top Level Domain Names (llTLD). The former are global in nature and the later country-specific. The examples of gTLD and ccTLD are **www.icaan.org** and **www.trai.gov. in** respectively.

(d) Internet Service Provider (ISP) : Internet Service Provider (ISP) is a company that provides access to the internet. The service provider giver a customer an internet connection that enables him to log on to the internet and browse in the world wide web and send and receive e-mail, etc. The Internet Service Providers (ISP) are themselves connected to one another through Network Access Points (NAPs). ISPs, also known as IAPs (Internet Access Provider), are a company that provides access to the internet. IAPs usually provide to its customers dial-up access through a modem and PPP connection. But some companies offer internet access through other devices, such as cable modems or wireless connections, etc. ISPs are mainly of three types, i.e., backbone provider, regional provider and local provider. The sender's information or message flows from computer to local provider then to regional provider to backbone provider and thereafter to another backbone provide to regional provider to local provider and finally the recipient computer.

(e) Web Portal : Web Portal, commonly referred to as a portal, is a service or a website that offers a broad array of resources and

services, such as e-mails, forums, search engines, online shopping, etc. Initially the web portals were online services, e.g., AOL, that provided access to the web, but now most of the traditional search engines have been transformed into web portals in order to attract and keep large users.

(f) Search Engines : Search Engine is an enquiry program that searches documents or information against specific keywords and returns a list of documents where the keywords are found. A search engine words by sending out a spider to fetch as many documents as possible. Another program, called an indexer, then read these documents and creates an index based on the words contained in each of the documents. The search engines used commonly and regular basis by the internet users are Google, Yahoo and Rediff.

- ***Internet Services***

(a) Electronic Mail (e-mail) : Electronic mail, commonly known as 'e-mail', is a method of transmission of messages over communication network. The message can be transmitted either through the keyboard or electronic files stored on the disk of computer. All online services and Internet Service Providers (ISPs) provide e-mails so that the users may exchange mail with each other through their systems. It takes only few seconds or minutes for a e-mail to arrive at its destination anywhere in the world and usually free of cost. This a very effective way to communicate with a group because you can broadcast a message or document to everyone in the group at once. Although different e-mail systems use different formats, there are some other emerging systems also, e.g., MAPI. Another X.400 standard has been developed by the CCITT that attempts to provide a universal way of addressing message.

(b) Electronic Business (e-business) : Electronic Business, also known as 'e-business', is the process of selling and buying products and services from or by a firm or business house, using computers and communication technologies. Such type of business includes different activities such as electronic payment, shopping, supply chain management, automation, selling goods like CDs, computers, etc. Some other firms sell services like consultancy, legal advice, technology training, marketing, etc. Sometimes a company may have an e-commerce but it may not have an

electronic business. Internet shopping is now becoming more and more popular. Consumer electronics, mobile phones and accessories, jewellery and watches and apparel all such items are now available in the online shopping basket.

(c) News Groups : 'News Group' also known as 'News Forum' or 'Forum', is an online discussion group that may be accessed through internet. There are several thousands of such groups available all around the world dealing with various topics of human interest on the internet. Some of the major television news networks, such as NDTV, CNN, ESPN, STAR and ZEE NEWS, provide such type of services. Sometime they combine the bulletin board service along with real time discussion or certain topic. This is a good source of information on a specific area of interest.

(d) Bulletin Board Service (BBS) : Bulletin Board Service is an another kind of service available on internet that allows a person to read the message left by other. The person receiving the message can reply to the sender by leaving his own message or the board. The Bulletin Board Service is an electronic message centre available on computer where one can reach through the network. Usually the BBS is a kind of platform where persons can share their views on a particular subject. Thus, this service is also a valuable source of information and sharing of ideas.

(e) Internet Chat : Internet chat means intercommunication of views, ideas and information between two or more users via medium of a computer network. In the process of internet chat, one user enters the message by typing through the keyboard and the entered message will appear on the user's monitor. Almost every network and online service provides the chat facilities for their users. A chat room is almost like a room where the chat takes pace. It is also termed as Internet Relay Chat (IRC) where a large number of people can engage themselves in real time communication. This service provides the facility of intercommunication between people living in the different parts of the world quickly with relative privacy.

(f) Instant Messenger : Instant Messenger is another kind of communication service available in the internet that enables a user to create a private room with another person. There are several instant messenger platforms available on the internet, i.e. Hotmail, Yahoo, Rediffmail, etc. Such types of instant messenger

service is quite poplar nowadays and allows the user to share their instant message and certain files with friends and family.[7] It provides instant service and the user can exchange the images, message, files, etc., within a minute and they can also update stock, news etc., make conversation through PC to PC and also play online games.

• *Electronic Data Interchange (EDI)*

It is a standard format used for exchange of business data. EDI may be defined, in other words, as a method of transfer of documents using predefined industry's standard between two or more computers. The ANSI X12 is the standard followed in such paperless business transmission, which has been developed by Data Interchange Standards Association (DISA). The EDI message contains a string of data usually presenting the facts, like price, product's model number, etc., separated by delimiter. Such string is known as a data segment. One or more data segments framed by a leader and trailor, form for a transaction set and it is the EDI unit of transmission, equivalent to a message. The parties or firms exchanging business documents through EDI transmissions are termed as the 'trading partners'. EDI is different from sending the e-mail or sharing files through a network. In the EDI system, the format of the transmitted documents must be the same for both the sender and the receiver. The documents transmitted are translated into a mutually agreed format by the software. An EDI usually consists of two parts—an outside envelop, and an inside envelop. The 'outside envelop' is like a usual envelop which contains a letter, etc., and the inside envelop may be considered as a letter or message. EDI is one of the various types of e-commerce which includes e-mail, fax, etc.

• *Networking*

(a) Intranet and Extranet : Intranet is also a kind of network used by an organisation. It also uses the same internet and web technologies such as TCP/IP (transmission control protocol/ internet protocol), HTML (hyper text markup language), XML (extensive markup language), etc., for collecting and disseminating informing within its officers and employees. An intranet is used to support e-commerce such as sales, customers, customer service and marketing, etc. The employees of a company can exchange internal information from one department to another department

in the company and can create their own web page or web sites. Hawlett Packard, VISA International, etc., are the companies which user intranet at a large scale.

(b) Local Area Network (LAN) : LAN is a kind of network used for connecting two or more computers and other computer situated within close distance such as within a building, an office or in a campus of business enterprise. LAN is privately owned and it does not use any kind of public communication or carriers. LAN networks are of two types—(i) Peer-to-peer Network (LAN), and (ii) Server based Network (LAN). The first kind of network, i.e., the peer-to-per network is comparatively easy to install and maintain because there is no central or dedicated server. It serves as a work station and allows the computers to share access to application like e-mail, files, hard discs, printers and modems.

The another kind of LAN, i.e., server based LAN, is a central computer which performs the function of server and provides application, communication, security and files services of such clients who are connected to LAN. Such type of LAN is suitable for heavy duty where a large number of computers are involved.

(c) Wide Area Network (WAN) : 'Wide Area Network' (WAN) is a computer network which is based on geographically dispersed telecommunications. WAN may be privately owned or rented. The term generally connotes the inclusion of public shared user network. The network operating in the geographical area of a metropolitan city is known as metropolitan area network (MAN). The working area of a WAN is not limited to a certain geographical area and it span may cover several cities or even countries. Computers and other devices in geographically remote areas are linked with the help of switched or dedicated corrections, which is not possible by LAN. The organisation providing service connections may be public or private.

- ***Technology Convergence***

The word 'convergence' may be defined as coming together of two or more disparate disciplines or technologies. The fax, for instance, is the result of convergence of telecommunication technology, optical scanning technology and printing technology. The information technology revolution including internet is the outcome of the convergence of telecommunication technology and computer technology. The convergence technology is nowadays

being increasingly used for various applications. It is the convergence that enabled us to access to internet through a mobile phone. The various electronic and electrical instruments along with their technological improvements have revolutionised the way of human life.

The Ministry of Information Technology, Government of India, had taken initiative to promulgamate a new law, i.e., Communication Convergence Bill in the year 2001, with an objective to promote, facilitate and develop and also for proper communications including broadcasting, telecommunications and multimedia. The bill, however, could not be passed due to certain unknown reasons.

Convergence of information technology has great potentiality in improving the utility of cyber space for applications in the human lives. It will help the business and commerce to grow substantially. In the meantime, there is also apprehension of its abuse for criminal activities causing dangers to the society. The criminals are also most likely to abuse such advanced technologies for enhancing their activities. The mobile phones has nowadays become one of the most potential weapons in the hands of criminals due to advanced additional facilities available on it. The use of cellphone in kidnapping case, MMS scam at Delhi, webcam porn scam at Pune, etc., may be cited as examples.

References

1. Concept of Information Technology, Aptech Limited, Mumbai, 1995.
2. *Chambers Twentieth Century Dictionary*, ed. A.M. Macdonald, 1973.
3. *The Times of India*, January 13, 2005.
4. www.kentlaw.edu/cyberlaw/resource/whatis.html
5. www.python.org/doc/current/lib/internet
6. www.icaan.org
7. www.yahoo.com; www.msn.com; www.newaol.com

3

Regulatory Perspectives and Technology

Synopsis

3.1. Impact of Information and Technology

The computer and network of information technology (IT) have become an integral part of day-to-day life. Its area and application is so broad that no human activities can be said to be remain untouched. Its application covers almost all the manufacturing and marketing sectors, viz., banking, communication, railways, tourism, education, agriculture, medical, administration, etc. The advent of Home PC and internet have further reduced the whole world into a small village communicable

from one part to another within seconds. The term Information Technology (IT) indicates all the aspects of managing and processing of information and useful human knowledges. The context may be presumed to be a small organisation or world itself. The word 'computer', as per Penguin Dictionary, defines the term as "a portmanteau phrase to cover all aspects of the art or science of processing of data to produce information". It covers computer software, hardware, programs, databases, semiconductor chips along with the process and produce of output.

The present advanced technology of information and communication provide wide and unlimited opportunities for economic growth and human development. It can enhance various development activities such as access to financial markets, employment generation, improved agricultural productivity, long distance education, tele-medicine, protection of environment, checking of pollution and management of disasters. It has potentially to help youth and women to grow by way of improving their capabilities and skills. It increases enormously the popular participation and enhances the decision making process at all levels.

The role and application of computers and networks in the human activities have increased tremendously after advent of internet. The little microchips are capable of storing huge valuable information regarding modern science and commerce. The industrial production of a company may be dependent entirely on the functioning of data system. The e-commerce is rapidly gaining popularity over the traditional form of business. Even in the field of medical science, IT is playing a lead role in diagnosis and treatment. With the help of IT, a doctor sitting in U.S.A. can supervise a surgical operation being conducted in Delhi or a person having chest pain in his car can seek medical advice from a cardio-physician. In brief, we may say that almost every sector of the world today is under substantial influence of the information technology in some or other way.

The advent of IT, however is not only boon but bane as well. The abuse of information technology is its negative side. It has provided new ways of opportunities to the criminals and anti-social elements. They are more able to expand their nefarious criminal activities in the cyber world. They are now applying

highly sophisticated ways and means of law breaking. They have now abilities to perform the traditional crimes in a modern way. A terrorist, for example, sitting in Pakistan can easily transmit his codified plan to Delhi within seconds with the help of internet. A hacker may transfer huge amount of money from one account to another or one bank to another within few seconds. There is possibility of secret information regarding nuclear energy, power production, satellite communication, defence, etc., being stolen by a computer expert.

The destructive activities relating computer networks may cost billions of dollars. The treat to network is in the terms of infrastructure, information and hosted-services and its possibility is widespread and low-cost access. Such loss of infrastructure in the cyber space is vulnerable due to three kinds of failure, viz., complexity, accident and hostile intent. The impact of such failure may be small and large. The increasing dependence of society on computer is increasing the dimension of such failure.

The term cyber space and its area includes internet, BBS, online services and other kind of services. It enables people to gather information computer networks using communication lines. Millions of people all around the world are now 'online' and connecting their personal computers for the sake of communication. Even the children are not away from the cyber space and more and more schools and Home PC are being connected with the internet. Several lakhs of people are communicating their feelings with their family, friends and relations using e-mail and chat services available in the internet. Businessmen all around the world are enhancing commercial activities through the network. The huge information available on internet is benefiting every walk of life and every strata of society.

3.2. Regulations of Cyber Space

A virtual mutual relationship and contact is established between persons who enter into the world of cyber space through their computers. Under the circumstance, persons who misuse the computer and network for ulterior motive and commit crimes affect such relationship and virtual contacts. Some people are of firm opinion that the cyber space must not be subjected to any outside interference.[1] Such opinion appears ideal from the idealistic viewpoint only. But the reality is not conducive to such

type of opinion. The regulation and control of cyber space has become essential because a large number of terrorist organisations all around the world are now using internet for terrorist activities threatening peace and tranquility of society and various nations. It is high time that now there must be an international regulatory body to watch the activities of cyber space, particularly internet, which is an anachronistic non-organisation platform consisting of millions of independent computers connected only through telecommunication channels and software protocols.[2] No country can remain a silent spectator to the concurrent happenings in the cyber space since the very existence, peace, law and order, etc., of such countries is under threat if such situation is allowed to continue unabated.

Some persons are the proponent of self-regulation theory. They are of opinion that the cyber space is a virtual entity and not amenable to territorial jurisdiction of any state or country. They suggest that the service providers and the vast community of online users of cyber space should form and manage their own self-regulating rules and regulations. The forms of self-governance is already in existence which include engineers engaged in developing technological protocols, sysops and access providers creating and imposing terms and conditions of access on their users and such ruler are commonly known as "netiquette". Additionally, cyber space already possesses some enforcement mechanisms, which include banishment from the server, flaming, shunning, mail bombs, or cancel bots.[3] The existence of ICANN may be an appropriate example in the context of self-regulation in cyber space. ICANN is an international non-profit and self-governed organisation which perform the responsibility of Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and Country Code (ccTLD), Top Level Domain Name System Management and root server system management functions. The Domain Name System (DNS) provides assistance to the user in finding their way around the internet. Every computer working with the internet has a unique cyber address referred to as "IP address" (Internet Protocol Address). Since it is difficult to remember the IP addresses (which are strings of number), the DNS provides a familiar string of letters (called the "domain name") to be used, such as www.icann.org. Different governments and international treaty organisation work

in partnership businesses, organisations and technically skilled persons are involved in manufacturing and maintaining the global internet within the whole structure of ICANN. In view of theory of maximum self-regulation in the high-tech economy, ICANN is perhaps the most appropriate example of self-regulation, running with the collaboration of various constituents of the internet community.[4] ICANN has proved the fact that internet can be regulated smoothly and properly even without any regulation from governments.

The success of self-regulation of cyber space is of course laudable but it fails miserably when the fact of serious abuse of networks comes before us, i.e., paedophilia, cyber frauds, credit card frauds, pornography, etc. Everyone knows that such types of acts are criminal acts, still these are occurring unabated. This is simply because no established system of criminal justice administration and penal provision are available so far to punish wrong doers effectively. Besides such crimes against individuals, there are several cases of defraud of huge money as well. The governments, therefore, are forced by the circumstances to bring legislation to check abuse of Net services and to avoid chaos and reign in the prospects of its development.

Besides problems of pornography, politics and privacy, there are financial aspects also such as taxation, intellectual property, trade, gambling, etc., which are needed to be controlled effectively. Some experts are of opinion that the criminal sanction should be exception and not the rule. In the matters other than criminal acts and public exchange, self-regulation and Netiquettes should be allowed to function and grow effectively and properly. The enactment of Information Technology Act, 2000 is a laudable effort of Government of India in this concern.

3.3. Legal Aspects of Regulation

There are some logistic problems in the wake of implementing legal regulations. The Net world may probably be divided into two worlds, i.e., real world and virtual world. The legal system of the real world functions on the basis of certain established assumptions and such type of functions are not applicable in the virtual world. To understand the problem, it is necessary to understand the meaning of the real world and the virtual world.

Real World and Virtual Word

'Real World' is a physical entity having well defined boundary demarcated and divided into sovereign states whereas 'virtual world' does not have any accepted requirement of the sovereignty. Real world functions on the basis of certain sovereignty of the nation states over its territory and population. But the virtual world, on the cyber space, does not conform to the accepted requirements of the sovereignty. It has no permanent inhabitants or population, no fixed territory and also no capacity to enter into diplomatic relations.

The concept of sovereignty, therefore, is not amenable to the virtual world called cyber space. The Net users enter into the cyber space by joining online and come out of the same by simply disconnecting. There is no permanent membership in the cyber world and any one can enter into it through connectivity. Even the highest regulatory body, ICANN, has very limited role to play. It is thus, obvious that it not easy to regulate the cyber space.

Legal Assumptions in Real World

State has got certain powers to enact a law or regulation in the case of sovereignty based nation or state. Such laws have a specific jurisdiction in the state to cover. The case of public and private international, however, may be taken up as exception. Even in the case of such international law, the enforcement has to be made by the agency of the state. The sovereign power to enact or law or regulation is always subject to a determinable geographical territory.

The law of the real world is enforced through the state's authority in a given territory. This principle of territoriality is widely accepted in the field of criminal justice system. Various states respect the existing laws of the land through mutual consent. If a country desires to enforce his law on a particular person, it has to obtain the sanction of concerned courts of the country to get the accused extradited. Such extradition becomes essential because a criminal prosecution generally requires the physical presence of the accused before trial court.

The legal system of real world construes property as some thing perceived, tangible and objective. The intellectual properties,

however, may be an exception. The principle of traditional legal system has a practical difficulty to adjust to the notion of digital or incorporeal property. The traditional law, therefore, may not deal effectively, for example, with theft case in the cyber world where a hecker steals a password or account number from a computer system.

In the transactions of the real world, the business and other legal relationship between the persons are made through the relevant terms and conditions written on a written document. In the field of cyber world, such type of paper transactions are not possible at all. Such type of relationship can be governed by electronic or digital records only.

The real relationship through the physical contacts are possible only in the real world. The essence of transaction is governed through the physical relationship, such as marriage, contract, offence of murder, etc. The traditional legal system is almost unable to deal with the increasing trend of virtual relationship emerging rapidly in the cyber world.

Legal Assumption in Cyber World

(a) World Unbounded : We have discussed earlier that cyber space is not amenable to nation-state theory which is based on the determinable boundaries and territorial limits. Cyber space is the space existing between two modems. Such electronic realm does not have any physical area or boundaries. Its areas covers to the extent of hardware such as computer equipment and telephone wires. It is situated where internet is located.

In internet, the information transmitted is broken into minute discrete packets of bit that can be transmitted as capacity permits. Packets are levelled with the address of their final destination, and may follow any number of different routes from computer to computer until they finally reaches their ultimate destination or at the place where recipient's machine reassembles them. Since the internet uses the packet system that may use numerous nodes situated in different continents to convey some information from one country to another and the boarder loses its significance. Information may be conveyed from one part of the world to the another part of world and it might happen that such transmission is illegal in one part and not illegal in another part of the world.

So the intervention through the state regulation may not be effective and successful.

(b) Global Enforcement : The offence under cyber space cannot be subjected to any one particular legal jurisdiction as the demarcation of cyber space under territorial boundaries is not possible at all. The offender sitting in one country may commit a crime in another country and even in several countries simultaneously. Sometimes, a number of countries may be involved since the transmission of message was accomplished through various other countries, with or without the knowledge of the offender. The legal action in each of that countries may vary and jurisdiction of one country may depend on the legal system of another country.

Thus, in order to find an effective solution of the problem, the enforcement of the cyber law should not be territorial but global. The representative of states or UNO should sit together and propose a internationally enforceable law. Such enactment is possible only through the cooperation and coordination at international level. Such law must have an extradition clause so that an offender committing crime in one country may be extradited to the country where prosecution have been launched against the offender. The ultimate aim of all combined efforts should be to control the cyber crimes based on globally accepted principles.

(c) Corporeal Property Unfounded :The traditional concept of property cannot be found in the cyber space as the property here is notional. After advent of internet, a new doctrine of criminal information is now emerging in the field of legal science. In this new approach, the legal concept and evaluation of corporeal objects differs considerably from the evaluation of incorporeal (information) objects. There is, however, an important distinction between information and data although both are technologically and legally relevant to each other. Information is a process or relationship that occurs between a person's mind and a stimulus. Whereas Data constitutes stimulus, i.e., electromagnetic impulse. Data are simply a representation of information or of some concept. Information is nothing but the interpretation that an observer applies to the data. Thus, the destruction or appropriation of data is the destruction of

representation and not the destruction or appropriation of actual information, idea or knowledge. The property is of notional value and information constitutes the core of property in the world of cyber space. The contents of web, domain names and graphic designs, etc., are the property (although incorporeal) in the cyber space.

(d) Virtual Relationship : The interactions in the cyber space acquires a distinction of virtual character on account of its accuracy, speed and the connectivity. The internet has a feature of anonymity and the message receiver cannot identify the sender unless he discloses his identity. It is also difficult to find out even the location over the Net. These characteristics provide virtuality to the relationship established in the cyber world and this situation makes it more complicated for the traditional legal systems to deal with the offences taking place therein.

(e) Digital Records : In the field of traditional legal system, the courts require physical evidence in the forms of things or records. But in the cyber world such evidentiary records may be found only in a digital form. Even these digital information may be partly in the number of computers and appropriate processing shall be necessary to make it into a single records. Thus, it is quite obvious that finding evidences in the case of cyber crimes will not be an easy job. The authenticity of digital records are another problem as such records are susceptible to change or tamper easily. Many countries of the world including India have enacted legislation to overcome such problems and provided legal recognition to technology based measures in authenticating digital records.

Cyber space is changing rapidly due to constant changes due to technological advances. The rules existing today have to change constantly because there is possibility of present rule becoming redundant tomorrow. No legal response may remain static for a long time. Global experiences shows us that new situation may compel a country to have a new law. The way Philippines enacted a new cyber law after the embarrassing incident of 'Love Bug' virus creation is an appropriate example to this aspect. The existing proesture of evidence presentation is required to be changed substantially in order to meet the new challenges.

References

1. Hamelink, C., *Human Rights in Cyber Space*, http : II www.religion_owline.org.
2. Delta, George, B., *Law of Internet*, Aspen Law and Business, 1997, New York.
3. Dr. Bakshi, P.M., *Hand Book of Cyber and E-commerce Laws*, Bharat Publishing House, New Delhi, 2001.
4. Walsh, (JJ), Cyber laws and Jurisdiction, htts : iiwww.geocities.com/jjwelsh1/cyberlaw.html

4

Technology and Forms of Cyber Crimes

Synopsis

4.1. *Influence of Technology on Criminality*

4.2. *Forms of Cyber Crimes*

- *Crimes Affecting Individuals*
  - *(a) Invasion of Privacy*
  - *(b) Voyurism*
  - *(c) Theft of Identity*
  - *(d) Cyber Stalking*
- *Crimes Affecting Economy*
  - *(a) Hacking*
  - *(b) Malicious Programmes*
  - *(c) Computer Sabotage*
  - *(d) Computer Fraud*
  - *(e) Computer Counterfeiting and Cheating*
  - *(f) Theft of Telecommunication Services and Mobile Cloning*
  - *(g) Copyright Infringement and Software Piracy*
  - *(h) Economic Espionage*
  - *(i) Tax Evasion and Money Laundering*
  - *(j) Cyber Squatting*
  - *(k) Internet Marketing Fraud*

- *Crimes Affecting Society*
  (a) Racial Propaganda
  (b) Pornography

4.1. Influence of Technology on Criminality

The fast developments in the field of technological advances, particularly in the field of electronics and information technology have ushered in a new era in the field of human lives. But such technological advances are not only boon for human beings; they have also brought some ill effects. Whereas the technological invention such as telephones, automobile, computer, cell phones, etc., have brought comforts and other facilities, on the other hand, it has created new opportunities for criminals and wrong-doers. A large number of young and misguided children are abusing internet and cell phones for fun but creating a lot of problems for others amounting to criminal offences. Many wrong-doers are now using a computer as a tool to facilitate unlawful activities and they are committing criminal acts such as fraud, the sale or distribution of child pornography, sale of drugs, etc., There is also large scale infringement of copy right and theft of intellectual property rights.

The rapid growth and application of internet is changing the ways of lives and also providing techniques to the criminals to operate in a new way. Internet, e-mail and such other devices provide many advantages to the criminals and terrorists all over the world. Advantage of anonymity provided by the latest communication modes like e-mail, chat rooms, etc., in the internet system permits criminals to operate freely. The organized gangs of criminals and terrorists all around the world have now new devices in the form of these systems in coordinating and widening their activities even beyond their respective national borders. Such criminals are even experimenting with the system to use it in a newer way to operate criminal activities.

The criminal abuse of telecommunication and information technologies for fun or otherwise have made all the aspects of human life susceptible to the criminals operating in the cyber world. For instance, if a computer hacker succeeds in tampering with the medical prescription of patient stored in the computer of a hospital, it may endanger the life of such patient. Such incident has really happened in U.K. where the life of 10 years old was

endangered in similar situation. Financial transactions being shifted at large scale by cyber criminals. Credit card frauds and ATM frauds are also now increasingly common. The privacy of people has not remained unaffected. For example, there years ago in Delhi, a senior television journalist decided to get cosy with her male colleague, when the duo went to withdraw money from an ATM. Their off-screen action was caught on the hidden camera and later circulated all over various TV channel offices.[1] In another well-known Anderson Tape Cyber Scandal, the private video of Pamela Anderson and ex-husband Tommy Lee having sex, was widely circulated online. These tapes are probably the most popular stolen video ever.[2] The law enforcement agencies and society have to face new challenges in tackling with the criminals operating in the evolution of criminality.

4.2. Forms of Cyber Crimes

It is of course not possible to give full and final description of various forms of criminal activities existing in the cyber space since criminals are experimenting continuously to find new methods of criminal act. The occurrences in the cyber world is unending and almost everyday we are witnessing a new form of criminality in the cyber space. However, we may discuss the types of cyber crimes prevalent today :

- ***Crimes Affecting Individuals***

(a) Invision of Privacy : The computers are nowadays most important source of preserving the personal as well as official data and personal information. It provides the ability to store, manipulate and transmit data much faster than any other systems of concurrent record keeping. Internet is now able to collect all kinds of information about a person, which he himself be not capable of. For example, when a person undergoes medical treatment in a hospital his entire medical history and data is fed into the computer of hospital. Likewise, a businessman keeps all information regarding his business transactions in his computer. Any person, authorised or unauthorised, capable of obtaining this data can make use or abuse of it.

The dangers of allowing the preserved data to flow with absolute freedom across the network may, of course, cause threat to the existence and privacy of an individual, an organisation and also the security of nation. The right of privacy is considered

as a fundamental right of the individuals in almost all the countries of the world. The availability of the data in the cyber space, through hacking or by other means with capability to access, may cause the criminal infringement of privacy. It also causes the infringement of the right of privacy enshrined in Article 21 of Constitution of India. The Hon'ble Supreme Court has categorically ruled that the right of life includes the right of privacy as well.[3] According to Article 12 of the United Nations Declaration of Human Right also, every individual has a right to privacy.

Experts are of opinion that unsolicited calls by bank, mobile companies, etc., for loan, credit card or even a new connection amounted to "enemic invasion of privacy of the subscribe of mobile telephony at all times and hours" and seriously impaired the fundamental rights of citizens. Nowaday mobile service providers and telemarkets are using at large scale the personal data of the subscribers for their business purposes as a product for sales promotion at the subscriber's personal and financial cost. Personal data given by a subscriber to a mobile telephone service provider should be treated as a confidential and there should be a law prohibiting service providers from transferring such personal data to other companies for commercial purpose. Recently Mr. Vivek Tankha, Senior Advocate of Supreme Court of India, in a PIL filed by him, has requested the Apex Court, citing a law in U.S. to ban such unsolicited calls, to issue directions to the government to enact appropriate law, scheme or regulation to protect mobile users "from this constant harassment and invasion of privacy through such calls".[4]

It is unfortunate that the Indian laws are virtually silent on the point of protection of privacy. Even the Indian Information Technology Act, 2000, which was enacted to "provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication", does not contain adequate provisions for the protection of right of privacy. The Act, however, contains a provision under section 72, which contains a provision for penalty for breach of confidentiality and in the limited context, where any person illegally and without the consent of the person concerned discloses any electronic record, book, register, correspondence, information, documents or

other such material to which he got access under any of the provisions of the Act or rules or regulations made there under. The section 72 reads as follows :

> "72. *Penalty for breach of confidentiality and privacy* : Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such electronic record, book, register, correspondence, information, document or other material to any person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees, or with both."

Besides section 72 of the Act, there is another provision under section 74 according to which it any person, who knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose, he shall punished with imprisonment up to two years, or with fine up to one lakh rupees, or with both.

The international organisation, namely, the Organisation for Economic Co-operation and Development, has issued guidelines[5] in 1980, calling upon the countries all over the world to adopt sound data protection practices in order to prevent unnecessary restrictions or transborder data flows. United Nations has adopted a set of guidelines[6] in 1990 for regulation of computerised data files.

(b) Voyeurism : 'Voyeurism' is "an act done by a sexual pervert who derives gratification from surreptiously watching sexual acts or objects". And the 'voyeur' is he who takes a morbid interest in such sordid acts. The provisions of section 67 and others do not cover fully the act of voyeurism within its sweep. This is one of the serious lacuna in the Indian Information Technology Act, 2000 with regard to the privacy of individuals in the country. If section 67 of Act is to be invoked successfully, the prosecution have to prove that the images captured by the accused were electronically published in the form of CD or transmitted on the internet.

Serious debate on the point of making the 'voyeurism' a serious criminal act under the provisions of Indian law have been started after the Pune incident. An accused, Mohan Kulkarni, a 55 year old Pune landlord, was arrested by Police for allegedly installing three web cameras in rooms rented to outstation girl students. The accused was charged under section 509[7] and 294[8] of Indian Penal Code only[9], although the provisions of the Indian Information Technology Act contains more stiffer penal action.

As against simple imprisonment up to 'one year' under section 509 of Indian Penal Code, the section 67 of Information Technology Act, 2000 provides for imprisonment up to five years and fine of rupees one lakh for a first conviction. In the case of a second or subsequent conviction the punishment escalates to ten years imprisonment and fine of rupees two lakhs. Even in the case seeking punishment under sections 509 and 295 IPC, conviction depends a lot on convincing arguments on behalf of the prosecution and interpretations allowed by the judge.

The Supreme Court of India first recognised in 1964 that the right of privacy is implicit in the Constitution under Article 21, which specifies the fundamental right to life. But the ruling applies only to the state and falls under the protection of Human Rights Act, which led to the formation of the national and state human rights commissions. In absence of categorical provision, there is general agreement among the law enforcing agencies that the hi-tech crime against woman would fall under the provisions of the IT Act, 2000 and *The Indecent Representation of Woman (Prohibition) Act, 1987,* and some sections of Indian Penal Code.

The provisions under section 67 of IT Act deals with offences of publishing or transmitting or causing to be published any kind of obscene information. Its ambit extends over information that is lascivious, or which appeals to prurient interests or if the effect is such as to deprave or corrupt persons who are likely to hear, see or read it. The IT Act oversides inconsistencies due to any other Act. Other law that deal with the issue includes section 292 of the Indian Penal Code, which covers sale and distribution of obscene information like brochures and pamphlets. Conviction may result in three year imprisonment and the fine determined by the judge. The Indecent Representation of Woman (Prohibition) Act, 1987 seeks to check this practice in advertisement,

publications, writing, painting, figures or any other manner. But the maximum penalty is just two years imprisonment and fine up to Rs. 2000.

The legal experts are of opinion that the present provisions of Indian law are not adequate enough. The advanced technologies, they say, must be used for fair purpose and in the cases where "the rights of the individual are infringed and unsuspecting individuals are filmed to cater to voyeuristic needs of others, the law should have stringent punishments like five years imprisonment not just for cameraman but also the distributor. They also suggest one change as needed in the IT Act, as under it only ACPs or Deputy Superintendent of Police (DSP) can investigate such crimes. This restriction is unreasonable as there is shortage of officers up to ACP or DSP rank and, therefore, such provision makes police resources smaller.

(c) Theft of Identity: The term 'theft of identity' or 'identity theft' usually refers to the acts of frauds, thefts, forgeries, misrepresentation of fact and impersonation, etc., involving the use of another person's identifying information. It affects the confidence in the integrity of commercial transactions and causes infringement of individual privacy. The acts of obtaining a credit card and loans in the name of someone else may be appropriate examples of 'identity thefts'. Such type of criminal act also involves the hiring of apartment, non-payment of bills, obtaining a cellular phone connection, purchasing a car, taking a home loan, etc. More serious type of 'identity theft' occurs when the thief commits a crime in the home of a victim and leaves behind a criminal record in his home. Internet has now become an easy, low-cost and efficient medium for capturing the identities of unsuspecting victims.

Since victim of identity theft is quite innocent and unknown to the act done in his name, he feels shocked and surprised when a creditor calls him to pay or police approaches him for the crime done in his name. It becomes very difficult for him to prove his innocence in a lawful manner. Such type of incident may occur due to negligence of the victim, who fails to protect his personal data preserved in his computer or due to lack of data security in computer where the data concerned of the victim is stored.

'SMS spoofing' is a latest form of cyber crime falling into the category of identity theft. In this type of crime, the criminal uses

a web-based software, states another person's identity in the form of his or her mobile phone number to send a message from a computer to some unsuspecting person. It appears to the recipient as if the message has been really send by the victim. It may happen that a wife receives a SMS from her husband demanding huge money to avert a trouble and as soon as she comes out of her house, she is attacked and robbed.[10]

(d) Cyber Stalking : Stalking is existing in our society since long. It is an act 'to stride stiffly or haughtily', or 'to approach someone under cover or without disclosing identity'. Stalking on telephone, particularly by children, is very common occurrence in our society. Initially, the characterised stalking was dismissed as minor incidents, not desiring any state or legislative intervention. Minor actions such as harassing telephone calls, unsolicited gifts, persistent chasing, etc., were either ignored or simply dealt with by the other provisions of law. The protection from Harassment Act, 1997 has been enacted by the United Kingdom. Nearly 17 states of United States of America have also adopted Anti-stalking legislations, to check stalking.

Cyber stalking is just another form of stalking in which electronic medium like internet are used to harass or contact another person in an unsolicited fashion. The term cyber stalking is used to refer only the use of electronic communications, such as internet, e-mail, SMS, MMS, etc., as a device to do stalking. The cyber stalking is usually anonymous and can be operated by anyone across the globe. It does not cause any kind of physical threat or harassment. There are wide variety of means of stalking by which an individual can harass others without sharing the same geographical border. It may present a range of physical, emotional and psychological consequences, which may sometimes be devastating to the victim. The menace of cyber stalking is increasing rapidly due to increasing number of people using internet in their day-to-day life.

- ***Crimes Affecting Economy***

The use of Internet for the sake of development of business and commerce is known as e-commerce. The large scale conduct of trade and business through the internet has enhanced the growth and development of new technologies and communication systems also. The speed and cost effectiveness are the major advantages. The

electronic commerce or e-commerce has enabled people to carry on their trade and commerce across the national border without any problem of time and distance. These technological developments, however, are not free from disadvantages. Since huge amount of money is being transacted for e-commerce, the criminals are bound to be attracted. The criminals armed with sophisticated technological devices have more easier ways to carry out their criminal activities. Today hacking is being used by the criminals at large scale to commit acts of espionage, software piracy, computer frauds and sabotage. The details of cyber crimes affecting economy may be summed up as follows :

(a) Hacking : The term 'computer hacking', broadly speaking, describes the act of penetration of computer system by way of manipulation, sabotage or espionage. The potentiality of hacking was realised by cyber criminals after large scale use of the computer networks by government, military and commercial organisations.

The hacking technique is dependent upon the respective communication and security system generally used by a network or computer. Hacking was traditionally committed by the use of standard password, watching physically the system or confidence tricks. After advent of internet, now new devices of hacking and computer manipulations are being used. Some of the major techniques used by the hackers are as follows :

(i) IP-spoofing : Through this technique, a person endeavours to make unauthorised access to computers or networks by way of pretending to be an authorised and trusted device inside the penetrated network. It is done through the modification of IP addresses in data packet headers transmitted to an incoming part of the network's router. The routers are not able to distinguish between data transmitted from outside or inside of network. Nowadays the newer routers and firewalls claim protection against this kind of attack.

(ii) DNS-spoofing : "Domain Name Service" (DNS) provides the service of mapping between host names and IP addresses. 'DNS-spoofing' is an act in which fake hotsmask are made during the resolution of internet. For any access on the internet, the name of host used has to be resolved to its IP address and this is done by communicating with a DNS-server which stores the hotsmasks

in databases. While doing the DNS-spoofing attack, hackers make efforts to intercept the communication and sends fake hostname mappings to the victim's computer. This can be done easily by using malicious web appelets downloaded by the attacked user himself. As soon as the applet is activated, the communication of user can be rerouted and the transmission data can be collected.

(iii) Web Spoofing : 'Web spoofing' is comparatively easier than IP and DNS-spoofing for which sophisticated technical knowledge is required. It is based on optical illusion in general where hyperlinks on web pages can contain characters that makes an address look like real, but in fact it lead to a wrong web site. For example, a hacker can create a wrong web site by replacing 'O' letter in the address www.micrsoft.com. Most of the user did not suspect any kind of malicious intention.

Kinds of Hackers :

(i) *Scamps* : The hackers do hacking only for fun and they have no intention to harm.

(ii) *Pioneers* : These are usually young chaps who are often fascinated by the emerging new technologies and explore it without understanding what they are actually going to find.

(iii) *Vandals* : Such hackers cause damages without any personal gain.

(iv) *Explorers* : Such type of hackers usually feel pleasure in breaking into computer system.

(v) *Addicts* : Such type of people are literally addicted to hacking and making abuse of information technology.

Legal Provisions in Indian Law

The section 66 and section 70 of 'The Indian Information Technology Act, 2000' makes hacking an offence, punishable within imprisonment up to three years, with fine which may extend up to two lakh rupees, or with both. The punishment, however, is more severe in the case of hacking done with protected systems. The said provisions are as follows :

"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."

and

"*70. Protected Systems* :

(1) The appropriate Government may, be notification in the Official Gazette, declare that any computer, computer system or computer network to be protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected system notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine."

It is important to mention that the Indian law does not intend to punish a hacker for an unauthorised entry into other's computer. It is punishable only when a hackers enter and thereafter "destroy or delete or alter any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means". Unauthorised entry is punishable only when such entry is made into a "Protected system", as defined under the provision of section 70 of the Act.

(b) Virus/ Malicious Programs : The malicious programs such as virus, worm, Trojan, Logic Bombs, Hoaxes, etc., are intended to cause harm to the victim's system. The details are :

(i) *Virus* : The virus is a malacious program which infects an executable file and causes that file to function in some way other than what was its original function. It has the ability to propagate itself attaching to executable files like application program operating system, macros, script, boot sector of a hard disc or floppy disc, etc. For example, an American student Jeffree Lee Parson was

arrested in August 2003 for creating a virus, namely, "MS Blast-B".[11]

(ii) *Worms* : The worms are malicious programmes which harms to multiply itself and send copies to others. Unlike virus, it does not alter or delete any files. It releases a worm into internet and causes slowing or clogging of network since the worms keep multiplying themselves, they affect and then starts sending copies to other computers. However, recently a worm namely "Klez" was detected in 2002, which has the properties of both virus and worm.

(iii) *Trojan Horse* : It is innocent looking program usually used by a hacker to collect data like passwords, credit card number, etc. Such program can either by transmitted by an outsider to the victim's computer or victim himself ignorantly can download it from some other computer assuming that it is a useful program.

(iv) *Logic Bomb* : It is also a malacious programme executable at a particular event. It marks the program to go into an infinite loop, crash the computer, delete data files or causes some other kind of damage to the computer or its data.

(v) *Hoax* : It is only a false warning regarding existence of some malacious program.

It is easier to send virus or malacious programs since the internet works on the basis of the interconnectivity of computer networks. Internet and e-mail are most common way to spread virus and malacious programs. For this, the distance is no longer a problem as entire world is now like a village.

(c) Computer Sabotage : The computer has assumed great importance as governments, companies and individuals are substantially dependent on computers for storage of valuable data. Gone are the days when sabotage was caused by physical acts of destroying computers by firing or bombing a building. Even the insiders have an opportunity to cause sabotage by using electrical short circuits or pouring saline solution over the hardware. Due to increasing dependence on computer network and information technology, there is possibility of computer threats and extortion as well. Since large scale valuable and confidential

information and data are being kept in the computer hard disc, the criminals have now an opportunity to steal these data and information and then resort to blackmail for extortion of organisation and individuals for unlawful gains.

(d) Computer Fraud : The word 'computer fraud' indicates usual economic offences that are being carried out by the criminals with the computer network and internet facilities. Initially the computer frauds were limited to the extent of manipulations of data, tampering of invoices, account balances, stealing of data, payment of salary, etc. With the advent of internet the computers are interlinked world over and hence the possibilities of committing fraud has increased beyond national borders.

Certain inherent features of internet, such as anonymity, cost-effectiveness, breadth of reach, difficulties in authenticating identity, etc., have made it difficult to check fraudulent acts. A fraudulent investment scheme looking credible and genuine may be put on advertisement all around the world within seconds and on negligible cost through internet and e-mail services. So it is much easier for a computer fraud to find gullible customers at large number through the Net services. The possibility of such fraud is obvious in the field of e-commerce also where goods and services are obtained online and payments are made through credit cards or such other based instruments.

Certain amendments have been made in the Indian Penal Code through The Indian Information Technology Act, 2000 to cover computer frauds under the purview of traditional frauds. Certain provisions are available against frauds in the Indian Information Technology Act, 2000 also. Section 65 of the Act contains, for example, penal provision for 'tampering with computer source of document'. Section 66 of the Act prescribes penal provision for 'hacking with computer system'. The section 71 and section 72 of the Act contain penal provisions for the criminal act of 'misrepresentation' and 'breach of confidentiality and privacy' respectively. Similarly, section 74 of the act prescribes penalty for publication of digital signature certificate for fraudulent purpose. Again, section 76 of the Act, prescribes specific procedures of confiscation apart from section 100 of C.P.C., of instruments used in the computer offences, such as computer, computer system, floppies, compact disks, tapes, drives and any

other accessories related threats. Similarly most of countries have either passed new legislations or brought amendments in their existing laws to make computer frauds punishable.

(e) Computer Counterfeiting : The computer counterfeiting is much similar to the computer fraud. The authenticity of any document relating to e-commerce is a matter of great importance for whole community. The advanced printing technology done through computer is helping criminals also in making counterfeit currency notes, judicial and non-judicial stamps. Digital technology provides perfection to such counter-feting of documents. Telgi stamp scam rocking whole Indian authority, may be taken up as an appropriate example. Fake Board and University degrees are also being prepared at large scale in different parts of the country.

The computer fraud and counterfeiting were earlier dealt with by the provisions of Indian Penal Code, i.e., 417 (cheating), 465 (forgery), 471 (using as genuine a forged document known to be forged), 467 (forgery of valuable security, etc., or to receive money), etc. But now specific provisions has been made under section 74 of the Indian Information Technology Act, 2000 to deal with fraud, forgery and conter-feting of digital signature only. The section 74 of the Act covers Digital Signature only and this is one of the serious lacuna in the IT Act. The provisions of section 74 read as follows :

> "74. *Publication for Fraudulent Purpose* : Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fire which may extend to one lakh rupees, or with both.

So, the Indian law have no adequate provisions to deal with forgery and fraud concerning with valuable documents done with the help of computer.

(f) Theft of Telecommunication Service and Mobile Cloning: The recent advancements in the field of technologies have now made telecommunication system highly dependent upon computer networks. The repeater system, exchange, mobile networks, etc., use the similar technology of computer networks. It is, therefore, easier for a hacker to invade into the communication network's

system to make their own fake calls or to provide free services to others. Such type of internet telephonic frauds are causing huge losses to the telecommunication companies all around the world.[12]

The rapid growth in the use of mobile or cell phones are providing another area for criminal operations. The criminals usually crack the code and connect the phone to the service provider and on misuse the same. 'Mobile Phone Cloning' is a latest form of crime adding a new dimension in the world of techno crimes. 'Mobile Phone Cloning' is a criminal act "where security data from a mobile is re-progammed into another mobile so that calls could be made from both phones but only the original would be billed."

Mumbai Police booked first-ever case of phone cloning recently. The accused, Vilas Tejam, was employed with LG phone service centre.[13] The firm of the 'accused, being an authorised service centre, regularly received phone handsets needing repairs. The accused, using software and equipment freely available on the internet, decoded the electronic serial numbers (ESN) and the MIN number from these phones and re-progammed them onto other phones. He used his personal floppy for saving the software and thus could not be nabbed for a long time. He used to rent out the cloned phones for a fee of Rs. 1,000 each. By this way, the SIM could be cloned again and again and used by a number of people while the bill would have been borne by the original user. The land phones and internet connected computer telephonic systems are also subject to similar type of attacks.

(g) Copyright Infringement and Software Piracy : Copyrights means the exclusive right of an author or producer of the art, etc., which empowers him to do or authorise others do certain acts for the publication or commercial exploitation of the copyright material, which may include a book, literary, dramatic, musical, paintings and such artistic works, and cinematograph film and sound recording, etc. Such right is considered to be *quid-pro-quo* and its the benefit accured to the author for the creation or intellectual property produced by him. Therefore, any kind of commercial exploitation of copyright materials by unauthorised persons amounts to a crime against the author as well as the society and is termed as "piracy".

The copyright piracy is one of the most common cyber crimes being committed in the cyber space. The protection of copyrights of authors or producers of a book, audio or video cassette, software program is one of the biggest challenge before the law enforcing authorities all around the world. The protection of intellectual property rights including of computer software, is essential for the continuance and development of our useful knowledge and life. It is imperative on the guardians of law to provide effective and adequate protection to the rights of authors so that they may expoit their intellectual products.

The advanced computer technology has made it easier to pirate the copyrighted works at large number quickly and at low cost. Due to large scale video piracy, for example, an original video CD of Hindi film of Rs. 200 is available in the market at the lower price of Rs. 20 only. The criminal acts of piracy has been encouraged and abetted at large scale by internet, since production being easier, even the risk associated with the physical distribution is also eliminated through online distribution. Apart from the software industry, film and music industry are among the most affected by the piracy. Even the very existence of music industry is under threat due to large scale availability of pirated copies and internet downloads.

The Copyright Act, 1957 has been enacted for the protection of copyright in India. According to the section 2 (O) of the Act, the term "literary work" includes computer programs, tables and compilations including computer databases. So, in the situation of violation of copyrights and software piracy a civil suit may be instituted to seek injunction and/or monetary damages and accounts of profits may be claimed. Besides civil proceedings, a criminal prosecution may also be launched under the provisions contained under sections 63-70 of the same Act.

(h) Economic Espionage : Commercial and business organisations are now depending largely on computers for storage and process of data and trade secrets. This dependence on computers has widened the scope of economic espionage in the cyber space. Several incidents of stealing of business secrets through hacking of reputed firms and selling it to the competitors are being reported all over the world. Both outsiders and the employees of such firms are seen involved in such type of crimes.

Sometimes the employee of commercial organisations are tempted by the competitors for purchasing the trade secrets. Sometime an outsider also performs hacking for obtaining trade informations for unlawful purposes.

(i) Tax Evasion and Money Laundering : Money laundering is an unlawful activity through which criminal proceeds take on the outward appearance of legitimacy. The criminals require to slash away their ill earned money and then invest it in another trade to have necessary legitimacy. For example, a notorious criminal in Mumbai, who earns money through extortion, is usually seen investing his black money in the film and the music industry of Bollywood. It is not easier to do money laundering in the traditional form through cash. Thus, the international criminals engaged in drug peddling, smuggling, etc., felt much difficulties in transferring huge amount of cash for the illegal trades. Under the circumstances, they use 'Hawala' methods in which a criminal sitting in Dubai can transfer money to Mumbai within few hours through the Hawala agents. For this, an agent at Dubai accepts cash at Dubai and sends message through internet or telephone in code words to deliver money to person concerned at Mumbai. As such, the money is transferred without any risk of interception or trap of law enforcing agencies.

Tax evasion has also become much easier after advent of e-commerce. Since the amount of the digital cash or e-cash kept in possession of a person is not traceable in the usual circumstances, it has now become almost impossible for a taxman or such other law enforcing agencies to have check on the income and expenditure of a person engaged in e-commerce. The traditional anti-tax measures and anti-money laundining mechanisms as well as legislation have become ineffective in different countries of the world after technological developments in the cyber space.

(j) Cyber Squatting : The cyber squatting is an act in which the site names in the internet are blocked and then traced by unscrupulous persons for monetary benefits. Reputed commercial organisations, celebrities and important government establishments are the main victims of cyber squatting. The United States of America has enacted a specific Act, namely Anti-cyber Squatting Consumer Protection Act, 1999, to check the criminal

act. The Act further amends section 43 of the Trademark Act, 1946 in order to fix up civil libability on the person who registers, traffics or uses a domain name. The Act further prescribes the penal provision for the offenders and the offender is liable to pay damages and profits, or statutory damages ranging from $1,000 per domain, as per discretion of the court.

(k) Internet Marketing Fraud : Net frauds are the newest form of cyber crimes spreading on web. Under its *modus operendi,* many fraudulent companies launch websites and seek members through the net. New members are charged a fee and asked to put more members to the network against certain commission. When the number of members becomes unmanageable, the companies shut shops and vanishes duping all members. The victim members loose the promised commission for introducing new members and initial amount paid. In two such cases registered with Delhi Police, the cheaters amassed a staggering Rs. 106 crore from more than 500,000 people.

(i) *Case 1* : A portal called www.bigbanyantree.com introduced an "earn while you learn" programme, where for course fee of Rs. 6,300, one could enroll for an online computer training programme offered by the portal. Each member was expected to introduce two others and, as the chain grew, member could there on earn up to Rs. 32,76,000 a year, just by introducing more and more people to the course.

On investigation, it was found that the computer course was not recognised by any government agency. Within three years, the company managed to enroll 5,00,000 members and collected more than Rs. 100 crore. Then, it suddenly decided to shut down the shop.

(ii) *Case 2* : M/s Bhasee Infotech Solution Pvt. Ltd. launched a website www.indya2net.com and gave out advertisement and brochures inviting membership to their marketing network.

After registration, which came at a fee of Rs. 13,500 (later increased to Rs. 14,580), members were routed to five different websites which had themes like i2nomatrimonials.com or i2ndoctors.com. Members were supposed to add details to the database by filling up

application forms and the company committed to pay each members Rs. 80 a day.

All this only lasted for about a year, after which the network burgeoned and the company lost track of its members. Then the promoters of the company went underground. The cheques they had issued started bouncing and the members were high and dry. As per estimates available with police, the company had duped about 5,000 computer professionals of over Rs. 6 crore by this time.

- ***Crimes Affecting Nations***

(a) Cyber Terrorism : Cyber terrorism is use of computers and cyber space for creation and propagation of terrorism. It is a recent form of terrorists act and such unlawful act which is done to intimidate or coerce a government or its people to press for fulfilment of political or social goals. In order to term it as cyber terrorism, it is imperative that an attack should result in threat or violence against people or property or nation, and/ or should cause fear of harm among affected persons.

The abuse of computer and internet networks for terrorists activities has caused threat of cyber terrorism over the security of national and international community. Computers are being used by government agencies for the shortage delivery and communication of valuable data of aviation, medical, defence, finance and financial services. Such valuable information are not free from outsiders' attack. They are vulnerable for being attacked by hackers and terrorists and the precious informations, if stolen, may cause disastrous effects on the security of respective nations. The thiefs of world today cause more severe damages to an organisation or a country with the help of a keyboard than a gun or bomb.

Terrorists are using the recent information technologies to formulate plans, raise funds, create propaganda, and to communicate message among themselves to execute a plan. For example, Doctor Nukher, a pro-Bin Laden hacker, is creating propaganda against America and Israel for the last five years. Another terrorists organisation, the Muslim Hacker's Club, is also operating in the cyber space since long. Al Kaida is one of the most notrious terrorists' organisation of the world and

operating throughout the world with the help of cyber space. Ramzi Yousef, the mothermind of the U.S.A.'s World Trade Centre attack, has also stored his detailed plans on the encrypted files in his laptop computer.

(b) Cyber Warfare : The role of computer by defence agencies in a war is another area of concern. The cyber warfare has now become an integral part of military strategies and most of the armies world over are now fully dependent on computer networks for all kinds of defensive and offensive operations. The threat of cyber espionage to gather information about the enemy's army and cyber attacks to immobilise enemy by way of destroying their information system, is looming large. The protection of computer containing Army's strategic details is a newer form of challenge before defence authorities. The question of protection from cyber warfare is also before the major international law authorities for being solved effectively.

(c) Unaccredited Calls : There are many unlawful agencies operating all over the world who are making unaccredited telephonic calls at international level causing loss to the exchequer of respective countries. When such calls are received by a person, no telephone number appears on the screen of caller Id of telephones. The telephone authorities such as BSNL and MTNL are failing miserably in India to check such calls, which have unearthed an international SIM cloning market which facilitated ISD calls between India and Saudi Arabia on cloned SIM cards.[12] The Delhi Police arrested seven persons along with a resident of Riyadh, Mohammad Aslam, who had been living in Delhi for the last three months for facilitating the illegal telephone operations.

In another incident, CBI arrested two engineers Ashok and Suresh who were engaged in the net-heist and making international calls as local one on the internet. Five exchanges were seized in Chennai and sleuths came across one such system at Hyderabad. CBI team found sophisticated electronic equipment connected to internet broadband lines along with mobile handsets, fixed wireless sets, routers, modems and other equipments. Using software based exchanges, they lifted international calls transferred into India through Voice Over Internet Protocol (VOIP or Net telephony) and delivered them into BSNL or MTNL network. Such operators

resulted an estimated heist of Rs. 400 crore to the BSNL and MTNL.

• ***Crimes Affecting Society***

(a) Racial Propaganda : The political leaders and their parties are often seen to utilise the computer and television network propagate their political agenda among people. The terrorists and antisocial organisations are also not far behind in making utilisation of computer and internet networks for creating social and communal hate propaganda among masses. For example, the Pakistani television networks is often seen creating political and social propaganda among the people of Kashmir in order to create indirect war like situation. With the global spread of internet services, the terrorist groups and other extremist organisations all around the world, have started using internet to propagate social and communal propaganda among their target group. Such type of damage is rather much more effective than the traditional methods of terrorism.

(b) Pornography : The propagation of pornography and paedophiles on the global internet is one of the worst abuse of computer and internet network. The internet networks have been made easy way for the paedophiles to organise and propagate the offensive and obscence materials throughout the world. The easy access to the suspecting children through the internets, to these paedophiles, makes them vulnerable exploitation.

The children have now easy access to the internet as more and more schools and houses are being connected to the internet. Such opportunity tends children to access unrestricted contact with inappropriate materials available in abundance on the Net. The students are most likely to be misguided by such materials which contains sexually explicit images or descriptions, pleads hate and bigotry, violence, drug abuse and such other illegal activities. Cyber criminals have now an easy opportunity to befriend a child in the chat room without disclosing his identity and than to exploit him. The internet, thus, has become very dangerous for children. However, it is not proper to keep children totally away from internet because a large number of useful information and educational materials are available on Net for the benefit of children. The beneficial things such as online friendships, pen pals, etc., are also available on net. The

appropriate step is the parental supervision on them so that they may misuse the internet and fall into the trap of paedophiles and bad elements engaged in promoting nefarious activities.

Section 67 of Indian Information Technology Act, 2000 contain a provision to check abuse of internet services. The said provision under section 67 reads as follows :

> *"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 material which is lascivous or appeals to the prurient interest or its effect is such as to tend to deprive and corrupt person 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."

The effective enforcement of aforesaid provision of law is not possible at all because the operation of internet can be done globally. An isolated effort at the level of a particular country cannot succeed. For the sake of rooting out this problem, an effective and efficient international effort is necessary. The technological innovation such as 'blocking of sites', 'child monitoring software', 'filtering software', etc. can be used to monitor and check children activities on the internet.

We, therefore, arrive at a conclusion that the cyber crimes are not completely new type of crime. They are almost traditional type of crimes but it is committed with the help of computer, internet, mobile, etc. Some addition are obvious coming into existence due to technological advances and the IT revolution. For example, mobile closing is new kind of crime which has taken birth after existence of mobile telephones. Since area of operation of cyber crimes is much wider, i.e., whole world, the affected parties may be found anywhere in the world and as such prevention and legal action must be ensured at world level.

Table 4.1

Indian Penal Code Provisons Governing Cyber Crimes

Sl.No.	Section	Offence	Penalty
1.	S. 292	Sale, distribution, public exhibition, etc., of an obsence object.	2 yrs. imprisonment and fine of Rs. 2000 for first offence and 5 yrs. imprisonment and fine of Rs. 5000 for second and subsequent offence.
2.	S. 294	Obscene acts, songs, etc., in a public place.	3 months imprisonment and/ or fine or both.
3.	S. 201	Destruction of evidence.	7 yrs. imprisonment and fine.
4.	S. 409	Criminal breach of trust (misappropriation of property) by banker, merchant, lawyers, etc.	Imprisonment for life, or imprisonment for 10 years and fine.
5.	S. 379	Stealing or theft of information.	3 years imprisonment, or fine, or both.
6.	S. 448	House-trespass (if accused has entered and installed camera, etc.).	1 year improvement or fine of Rs. 1,000 or both.
7.	S. 509	Words, gestures or acts intended to insult the modesty of a woman or intrude on their privacy.	Imprisonment for 1 year or fine or both.

References

1. *The Times of India*, January 15, 2005.
2. *Ibid.*
3. Mr. X Vs. Hospital 'Z' = 1988 AIR S.C.W. 3662; State of Maharastra Vs. M.N. Mardikar, AIR 1991, SC 207; People's Union for Civil Liberties, V. Union of India; Kharag Singh Vs. State of U.P., 1964, ISCR, 332.
4. *The Times of India*, Patna, February 8, 2005.

5. Guidelines of OECD for protection of privacy and transborder flows of personal data, Paris, 1980
6. UN General Aseembly, Resolution No. 45/95, dated 14 December, 1990.
7. Sec. 509 IPC, "Word, gesture or act intended to insult the modesty of a woman".
8. Sec. 294 IPC, "obscene act and songs".
9. *The Times of India*, Patna, January 14, 2005.
10. *The Times of India*, Banglore Edition, July, 2004.
11. *Hindustan* (Daily), January 30, 2005.
12. *The Times of India*, February 3, 2005.
13. *Hindustan* (Daily), January 30, 2005.

5

Computer Crimes and Cyber Crimes : A Criminological Analysis

Synopsis

5.1. *Computer Crimes and Cyber Crimes : Terminological Aspects*
- *Computer Crimes*
- *Information Technology Crimes*
- *Computer Related Crimes*
- *Telecommunication Crimes*
- *Cyber Crimes*

5.2. *Opportunities to Cyber Criminals*

5.3. *Motives of Offenders*

5.4. *Problems Affecting Prosecution*
- *Non-reporting and Negative Propaganda*
- *Outdated Criminal Justice System*

5.5. *Cyber Crimes : Challenges of Prevention and Control*
- *Checking the Opportunities*
- *Reducing the Motivations*
- *Challenges Relating to Guardianship*
- *Computer Forensic and Digital Evidences*

5.6. *Need and Prospects of Criminological Research*

5.1. Computer Crimes and Cyber Crimes : Terminological Aspects

Increasing influence of computers and information technology in the day-to-day affairs of the society have given birth to many innovations in the crimes and the scope of terms like 'computer crimes', 'cyber crimes', etc., widened. Due to rapid increase in the unlawful activities associated with the computers and networks, the existing term popular in use proved insufficient to indicate their gravity properly. The basic and the very concept of "abuse of computers" had different connotations for different agencies such as parliamentarians, law enforcing agencies, judicial officers, public forums, criminologists, sociologists, etc. The understanding of the word 'criminal act' may be entirely different for a hacker and a victim. Similarly, the use of the term may accordingly also depend upon the fact as to who is using the term.

The survey of information technology texts gives up many terms which are used commonly for description of the misuse or improper use of computer, computer related scientific equipments, i.e., cell phones, etc., and information technologies. The meaning and concept of 'computer abuse' is still construed different by various sections of people. There can be no one and single term that is capable of conveying the entire spectrum of improper activities in the computer or cyber world. The following are the terms used commonly in this context :

- ***Computer Crimes***

The word 'computer crimes' is used to indicate abuse of computer and it networks. It is the of one oldest and most commonly used terms. There are many activities which are yet not punishable in the eye of existing laws still to be included in the purview of the term 'computer crime'. Some experts are of opinion that for commission of a computer crime, the knowledge of computer is essential. The hardware used in a computer crime is nothing but a tool or an object of crime.

In view of recent developments in the information technology, the experts are of opinion that the knowledge of information technology is no longer an essential feature of computer crimes. The use of computer in society is so wide that the gap between knows and know-nots has no longer been in existence. Even a lay

man having little or no knowledge about computer is now seen being indulged in computer crimes.

- *Information Technology Crimes*

Some authors have been seen using the term 'information technology crime' for the sake of denoting the role of technology in the criminal activity. Some others are seen using the term 'Hi-tech crime' in order to denote criminal behaviour related to computer and similar other sophisticated criminal activities including the satellite communication system.

- *Computer Related Crimes*

The term 'computer related crime' was found to be in common use during the earliest period computer. The term was used to indicate the crimes being committed in relation to the computers and computerisation. The term, for instance, can be used to denote unlawful activities such as software piracy or hacking which has come into existence soon after the birth of computer itself.

- *Telecommunication Crimes*

The demarcating line between computer technology and the telecommunication technology has been obliterated after the arrival of cell phone, internet and world wide web. The telecommunication systems works with the help of computer systems and computer networks functions with the help of telecommunication system. Even the latest and most popular form of telecommunication system, viz., cellphone, functions with the computer technology. The term 'telecommunication crimes', therefore, has lost its significance in the present context. The significance and relevance of the word has been relegated to the level of minor crimes such as theft of cables, poles, equipments, willful damages, etc.

- *Cyber Crimes*

The large scale use of internet and computer network in the day-to-day human lives have made the subject of computer related crimes a matter of interest and popularity among the media and the common popular. The people of modern days are now increasingly dependent upon the computer and its applications. Amidst the increasing popularity of computer, a lucid term 'cyber' has caught up the imagination of people. Anything associated with the internet and computer network was called with a prefix

'cyber' and a lot of words came into existence—cyber laws, cyber cafe, cyber police, cyber space, cyber slaking, cyber fraud, cyber technology and so on. The information in the cyber space simply denote the activities in the virtual world or whatever 'online'. Thus the computer crimes rationed a new name and became 'cyber crime'.

Cyber crime may be defined as the "act of creating, distributing, altering, stealing, misusing and destroying information through the computer manipulation of cyber space; without the use of physical force and against the will or the interests of the victim".[1] The said information can be in any form ranging from electronic money to government secrets, and the victim can be an individual, a corporate person, or as defined in criminal law the state or society as a whole.[2]

The ambit of the word includes all kinds of objectionable or unlawful activities, misuse or abuse that are taking place in the cyber world, or through or against the computer and networks as well as telecommunication networks run with computer system or technology. The meaning of the word may vary with the variation in the facts and circumstances of each case. Every objectional activity, civil or criminal, causing adverse effect in the real world comes under its purview. The ambit of cyber crimes are bound to increase in view of ever increasing technological advances in the field.

5.2. Opportunities to Cyber Criminals

The growth of internet and cyber space is continuous and ever increasing. The wide connectivity, speed and accuracy of cyber space has reduced the whole world virtually into a small world. Every walk of world today, such as banking, insurance, stock exchanges, telecommunications, entertainment, electricity, judicial forums, nuclear installation, health care, legislation, administration, traffic control, air services education and others, are virtually dependent on the computer network for the sake of efficient services. Besides providing tremendous services to human kinds, the computer network and cyber space is providing disastrous opportunities to the criminals also.

The factors that contributes to the vulnerability, as identified by United States Manual on the Prevention and control of computer crimes, may be summed up as follows :

(i) Density and Storage of Information and Process : The storage technology allowing huge quantity of data provides opportunities to the criminal and hackers who want to steal, corrupt or destroy the data on a click of mouse. The centralisation or storage of information and processing system rendering an attractive opportunity to the infiltrators who are intending to attack the functions or information assets of an organisation.

(ii) System Accessibility : The security was not at all common at the initial stages of development of internet and the real object was to connect it to the large masses intending to use it. The unrestricted access to the system provides an opportunity to hackers to gain an easy access into the systems and create a lot of problems. Due to increasing activities of hacking, the problem of encryption and security is becoming a matter of serious concern among the computer and internet user population of the world.

(iii) Complexity : The operation of the system of cyber space is done by the support of local batch, remote batch and real time user modes. The typical operating system contains about 200,000 to 25 million individual instructions. It is can be said that such system are not fully known by anyone including the engineer designing it. An expert infiltrator can take advantage of the uncertainties created by the system complexity. The incidences of violating of security system have been reported where deliberate attempts have been made to confuse operator, or to interrupt systems by attacking little-known weaknesses.

(iv) Electronic Vulnerability : The computer system based on electronic technology are subject to problmes of reliability, fragility, environmental dependency and also vunerability to interference and interceptions. Such type of vunerabilities extends to whole communication network including telecommunication, in operation. The various traditional forums of electronic abuse, such as wire tapping, bugging, eavesdropping, analysis of electromagnetic radiations with the help of equipments, monitoring of cross-talks with adjacent electrical circuits, etc., can still be done by the criminals.

(v) Vunerability of Data Processing Media : The contents of most of the EDP media are not visually readable and therefore, the personnel processing the valuable data often handle the sensitive and secret files without being aware with the facts

contained therein. For this reason, the control of data items becomes a problem sometimes. There is possibility that even scratched topes, discarded CD or DVD may contain valuable information requiring special attention. The access to such information and utilisation may result into the easy penetration to many well-publicised systems.

(vi) Human factors : The employee working in various organisations are the most vunerable source of leakage of secret and valuable informations of such organisations. Such employee often fall prey to the hands of cyber crimes for money or similar other considerations. The personnel has the day-to-day access to sensitive data and sometime they misuse their position for extraneous consideration which includes the satisfaction of personal grudges or sevenge with the management or senior officers. The reason of threat may be malacious or subversive activities or for genuine effort, but human aspect is rather the most vunerable aspect of EDP system.

5.3. Motives of Offenders

We may say that there are many inherent factors that attract and facilitate their activities in the cyber space. Sometime for money and some other times for fun, but the criminals are bound to be attracted towards the cyber world. Cyber criminals have no dearth of motivation for committing crimes. The advantage of anonymity is the most advantageous among them. The motivational factors of cyber world are the similar to that of traditional world of crimes. They could be greed, lust, power, revenge, adventure and desire to taste the "forbidden fruit".[3] Unlike perpetrator of a traditional crime, the greed of money or similar monetary lust may not always be a factor of motivation. The motive in the cyber world may be malice, mischief or revenge and fun also.

5.4. Problems Affecting Prosecution

For several reasons anonymity of offender, distance being global, etc., there are several problems that hampers the success of prosecution concerning the cyber crimes. The problem becomes more serious as the system owners fail to take precautionary measures to avert any possible attempt to commit a crime against his system. Some relevant factor are :

• *Non-reporting and Negative Propaganda*

The lack of awareness among victim and people, non-reporting of incidents of cyber crimes and negative propaganda are the factors that hamper the success of the prosecution. The lack of awareness is seen not only among the people but various organisations and government agencies also. Negative publicity is supposed to be one of the main reasons for non-reporting of cyber crimes to law enforcing agencies. The reason of disreputation and fear of the competitive status in market being affected prevent the victims to avoid publicity and even to approach the law enforcing agencies and this results leaving of offenders free. The non-reporting deprives others to know the dangers and repercussions of cyber crimes.

• *Outdated Criminal Justice System*

Traditional criminal justice system is not capable to deal effectively with the well-equipped and sophisticated technologically advanced criminals operating in the cyber world. The traditional law, procedure, investigation and manner of presentation of evidence in the trial courts are unable to tackle with nature of crimes being operated in the cyber world. The law enforcing agencies also are unable to investigate the cyber crimes and collect evidence properly for the want of necessary technical knowledge. The positive efforts at international level must be made to educate the law enforcing agencies the technical knowledge concerning information technology. Since the area of operation is global, the investigating agencies must have the international relations and mutual cooperation for the sake of quick, effective and proper investigation. It is essential because the solution of cyber crime can only be found at international level and not at the level of respective countries.

5.5. Cyber Crimes : Challenges of Prevention and Control

It is apparent from our previous analysis that the opportunities, motivation and absence of effective preventive measures are the major factors that contribute to the birth, growth and expansion of cyber crimes. The following are basic problems concerning prevention and control of cyber crimes.

• *Checking the Opportunities*

The positive efforts in the wake of checking the opportunities

for cyber crimes is one of the most effective measures, which will nip the cause in the bud. The possibility of online crime increases as soon as a system is connected to the internet. But disassociating totally from the internet, for anyone in the present days situation, is very difficult in view of our increasing dependence on the information technology. The only solution, therefore, is to manage the risk involved in being connected to the cyber space, in such a way as to achieve the maximum benefits, which flows from the technologies.[4]

Only counter technological and scientific measures can succeed as cyber crimes are technology-oriented. Several technological devices are available limiting the opportunities of cyber crimes. The unauthorised access to the information and communication system is the initial step of a cyber criminals. So technological devices should be utilised to check their access. For example, the Supreme Court of India has adviced to the Government of Bihar to install mobile jammers in Bihar jails so that the criminal in jail may not operate their gangs telephonically for kidnappings, extortions, etc. Besides installation of jammers, the court directed the telecom companies to very addresses of applicants properly before providing connections to them.

Cryptographic technologies are well recognised as an essential tool for ensuring security and trust in electronic communication.[5] Digital signature and 'eneryption' are two important applications of cryptography. Digital signatures can show the origin of data (authentication) and further verify whether data has been altered or not (integrity). The encryption further helps in keeping the communication confidential. Confidentiality is essential because the criminal usually attacks in three phases. First of all, a hacker gains an access to an account on the target system, and secondly, he exploits vulnerabilities in order to gain priviledged access to the system and, finally, he uses the privileged access to attack other systems across the network.

Rule 7 of the Information Technology (Certifying Authorities) Rules, 2000 prescribes the standard architectures for different activities associated with certifying of digital signature in India, for e-commerce as well as e-governance purposes, though it allows certifying authorities to support open standards and accept real standards.[6] (See Table 5.1)

• *Reducing the Motivation*

Like other forms of traditional crimes—greed, lust, revenge curiosity, fun, etc., are also the motivational factors of cyber crimes. These factors cannot be checked fully because human nature is not amenable to effective control. The basic challenge is to accept the challenge of defeating a complex technological system. These human motivational factors are very difficult to change, except some minor changes through the awareness and awakening of moral ethics. It is, therefore, necessary that a credible guardianship and awareness campaigns should be adopted, apart from reducing the opportunities through adaptation of technological measures. Only the effective guardianship, awareness and use of the technological measures by the law enforcing agencies and justice administration can cause appropriate deterrent effect against motivated individuals from being indulging in cyber crimes.

• *Challenges Relating to Guardianship*

(a) International Cooperation : The area of operation of cyber crime is borderless and a criminal at U.S.A. can easily target a victim in India. The international cooperation, therefore, is necessary because the jurisdictional issues severely hamper investigation and prosecution of transnational cyber criminals. The international cooperation is necessary in several areas such as harmonisation of legislation and policy, surveillance and standardisation of investigation, agreement on extra-territorial jurisdiction, extradition of criminals, retention of witness and evidence and, finally, exchange of information. A close link between experts of information technology and law enforcing agencies is also necessary to ensure the prevention and investigation of cyber crimes with the help of recent technological developments and forensics.

(b) Legislative Measures : Appropriate legislative measures should be taken at international level for enactment of substantive law defining caterigocally the procedural laws, provisions relating to search and seizure, surveillance measures, extradition, international cooperation, etc. The Council of Europe Convention on cyber Crimes is a proper step in the field. Positive legislative measures may be initiated through U.N.O. also.

(c) Capable Investigating Agencies : The traditional police system is not capable enough to investigate cyber crimes because

of lack of technical knowledge, involvement of new techniques and digital evidences etc. There is urgent need to increase their capabilities at individual level so that the investigating agencies tackle cyber crimes in effective manner. More technically proficient team of officers may train others in retrieving and analysing the digital evidences in professional manner, so that their evidentiary value may not be affected or lost.

The recent technological advances in the field of information technology has opened up new opportunities as well as challenges for the law enforcement agencies. If the criminals have an opportunity to continue their criminal activities on the internet, than the police can also avail the internet facilities to monitor and trace such activities. Criminal and usually quite proficient in exploiting the advantages of Hi-technology and, therefore, now policemen should also develop their capabilities to outsmart by improving their technical knowledge and style of functioning.

- ***Computer Forensic and Digital Evidences***

Computer forensic, also known as computer forensic analysis, is one of the fastest developing knowledge in the field of criminology. It involves the processes of electronic discovery, electronic evidences discovery, digital discovery, data discovery, computer analysis and examination of computer media, viz., hard discs, diskettes, tapes, etc. for evidence. A skilled computer and forensic analyser can reconstruct the activities of a computer user. The task investigation in cyber crime is a matter of technical competency and there is possibility of evidence being destroyed by a traditional investigator. The investigator must know how to ensure safe collection and custody of evidence for analysis by the computer forensic.

5.6. Need and Prospects of Criminological Research

The growth and development of information technology in India is much faster than many other countries of the world. IT has become one of the most integral part of the country's economy. Administration and legislative efforts are afoot to ensure positive development in the field of IT. India has become third largest manufacturer of IT equipments in the world. Police has started using latest IT technological devices to bust gang of criminals and check the criminal activities.

In view of increasing importance and applications of IT, there is an urgent need to include cyber crimes in the curricula of criminological studies in law colleges and universities. The research works on cyber crimes based on case studies and data should be encouraged so that the investigating officers and agencies may have appropriate knowledge on the point of concurrent motives, *modus operandi*, etc., concerning cyber crimes. In this field, Asian School of Cyber Laws have made commandable effects. The school made comprehensive studies in the field and analysed 6,266 incidents of cyber crimes and IT abuses within two years' period, i.e., January 2001 to December 31, 2002.[7] It is , therefore essential that research works of various aspects of cyber crimes be encouraged in the context of Indian milieu.

More and more people are using internet and other cyber facilities. A large number of people and organisations are putting their confidential and personal data and information stored in computer that are connected to internet. Such users under constant threat of hackers, who may misuse such information. It is, therefore obvious that unless the awareness level is raised among common masses such possible misuse of cyber crimes are bound to increase.

The availability of authentic data is very important for criminological researches. In the foreign countries like U.S.A. and U.K., a number of computer security surveys have been conducted during the past years, but such efforts are still awaited in India. The lack of such type of survey and inferences of criminological observations with further result in the dearth of availability of sound criminal justice statistics on computer crime. The criminological inferences and datas available in the context of foreign countries are not effective in the Indian context. So, in order to know the exact nature and extent of the problem in India, we must conduct separate surveys and obtain authenticated cyber crimes vistimisations finding. There is also necessity to develop research tools and methodologies to understand the control of cyber crimes, thus must be appropriate coordination between of curricula and research, technology based security measure and people operating of cyber crimes.

Table 5.1

Sl.No.	The Product	The Standard
1.	Public key infrastructure	PKIX
2.	Digital signature certificate and digital signature revocation list	X. 509 version 3 certificates as specified in ITU RFC 1422
3.	Directory (DAP and LDAP)	X500 for production of certificates and certification revocation lists (CRLs)
4.	Database Management Operations	Use of generic SQL
5.	Public key algorithm	DSA and RSA
6.	Digital Hash Function	MDS and SHA-1
7.	RSA Public Key Technology	PKCS # RSA Encription Standard (512, 1024, 2048 bit) PKCS # 5 Password Based Encryption Standard PKCS # 7 Cryptographic Message Syntax Standard PKCS # 8 Private Key Information Syntax Standard PKCS # 9 Selected Attribute Types PKCS # 10 RSA Certification Request PKCS # 12 Portable format for storing Transporting a users private keys and certificates
8.	Distinguished name	X.520
9.	Digital Encryption and Digital Signature	PKCS # 7
10.	Digital Signature Request Format	PKCS # 10

References

1. Joga Rao, S.V., *Law of Cyber Crimes*, 2004, p. 70.
2. Cyber Crime; A Challenge to Leviathan : http : 11 www.ise.ac.uk/clubs/havek/essay/cybercrime
3. Kataev, Dr. S.L., "Criminalistic and Social Aspects : Cyber Criminality"; www.crime-researchorg./eng/library/kataev_1_eng.htm
4. Grobosky, Peter, "Computer Crime : A Criminological Overview", Australian Institute of Criminology, 2001, www.aic.gov.au.
5. OECD Guidelines for Cryptography Policy.
6. See Rule 7 of the Information Technology (Certifying Authorities) Rules, 2000.
7. Computer and Crime Abuse Report, India, 2001-2002, Asian School of Cyber Laws, March, 2003.

6

Cyber Crimes and Global Response

Synopsis

6.1. *Global Perspective*

6.2. *Countrywise Legal Response*

6.3. *Countrywise Analysis in Brief*

- *United States of America (U.S.A.)*
- *United Kingdom (U.K.)*
- *Australia*
- *Austria*
- *Belgium*
- *China*
- *Estonia*
- *Germany*
- *Ireland*
- *Malaysia*
- *Malta*
- *Mauritius*
- *Philippines*
- *Romania*
- *Singapore*

6.1. Global Perspective

One of the most important distinctive features of cyber crime is that its impact is much wider than the traditional crime. A criminal act committed in one part of the world may cause impact at some other part of the world. In view of reach of the cyber crime, entire world has virtually turned into a small village. Another feature is that the criminalisation and increase in the cyber crime is uniform all around the world. It may happen that an act is a crime in one country, but may not be in another country. But if a person commits a crime, although it may not be crime in his country, he still may be liable to prosecution under the provision of law of another country. For example, if a person in U.K. sends virus to a person's computer in India, he may be prosecuted in India. Thus cyber crime has got the omnipotent characteristic and therefore, it can have victims anywhere in the world. It is now essential that all those persons, who deal with cyber world, must have some idea about as to what acts constitute cyber crime in the different countries of the world.

Since impact of cyber crime is unbounded, any effort made at national level have to meet international coverage for the sake of effective containment of cyber crimes and protecting the interest of the society at large. Such situation necessitates understanding of global legal response relating to the cyber crimes. The discoveries and inventions, both constructive and destructive, are very rapid all around the world. In absence of international cooperation, it will not be possible for any country to know the recent advances in the other country. A country victim of any kind of latest cyber crime shall have the opportunity to intimate other countries in time so that it may plan its defence well in advance. An attempt is being made here to briefly introduce the salient features of various statutes of world.

6.2. Countrywise Legal Response

The legal response to the cyber crimes of various countries of the world are varied. Such laws are still under its gestation period. There is not even a single law that can be stated to contain all the necessary attributes of modern cyber legislation. For example, unsolicited calls by telemarketers and others are supposed to be an infringement upon the right of privacy and liberty of a person, but no provision for such act is available

under the Indian IT Act and rules. The U.S.A., however, have implemented a special law for the purpose about 13 years ago and several European countries follow the U.S. model to provide a safeguard to consumers from being harassed by cell phone companies and telemarketers. Some of the representative legislature efforts made by the various countries of the world are being discussed here.

United Kingdom, followed by Austria, is rather the first country to initiate the legislation in the field of cyber world. The United Kingdom have enacted *'The Computer Misuse Act, 1990'* which contains penal provisions for cyber crimes. The country thereafter enacted *'Regulation of Investigatory Powers Act, 2000'*. Austria thereafter took steps in the field and amended its existing laws through enactment of *'Cyber Crime Act, 2001'* to check cyber crimes. Belgium also amended existing laws in November, 2000 and made computer forgery, sabotage, computer fraud and hacking criminal offences. China also promulgated *'Computer Information Network and Internet Security Protection and Management Regulations, 1997'* to regulate internet activities, but major stress was on the national security rather than prevention of cyber crimes. Criminal code of Estonia contains certain provisions governing cyber crimes.

German Penal Code also contains certain provisions applicable to crimes committed with the help of computer and computer networks. Ireland has enacted *'The Criminal Damage Act, 1991'* containing specific provisions on damages caused to or by a computer system or network. *'The Computer Crimes Act, 1997'* of Malaysia deals exclusively with crimes relating to computers. Malta enacted *'The Electronic Commerce Act, 2001'* for regulating electronic commerce and the Part VII of the Act contains amending provisions with regard to 'Computer Misuse' for being incorporated in the criminal code of the country. The Penal Code of Mauritius has relevant provision governing computer related crimes. The country has enacted also *'The Information Technology (Miscellaneous Provision) Act, 1998'* to check cyber crimes. Besides these laws, there is *'The Economic Crime and Anti-Money Laundering Act, 2000'* to deal specifically with money laundering.

Romania has adequate provisions of law governing cyber crimes and other related criminal activities. The country's Title III

is. Anti-corruption law and Law No. 676 and Law No. 196/2003 respectively governs "the process of personal data and the protection of privacy in the telecommunication sector" as well as "preventing of pornography". *'The Computer Misuse Act, 1998'* of Singapore deals exclusively with the cyber crimes. Similar provisions are available in the United Kingdom's *'The Computer Misuse Act, 1990'* also. United States of America (U.S.A.) has the widest range of legal provisions concerning cyber crimes. It has passed several legislations containing provisions relating to computer and network misuses. There are certain provisions in Federal Code also. Individual states have also enacted there specific and separate laws on the issue.

6.3. Countrywise Analysis in Brief

- ***United States of America (U.S.A.)***

U.S.A. has passed several enactments which cover various aspects of cyber crimes. Various states have also made federal enactments of the issue and it is not possible to discuss these multiple and varied federal laws here. These Federal Acts, however, are either to introduce or amend an existing provisions in the U.S. Federal Code. The major provisions of U.S. codes governing criminal activities in cyber space is as follows :

(a) Federal Criminal Code Concerning Computer Crimes :

- — 18 U.S.C. S 1029, Fraud related activities in Access Device.
- — 18 U.S.C. S 1030, Fraud related activities in connection with computers.
- — 18 U.S.C. S 1362, Offence relating to communication lines, station or systems.

(b) Federal Statutes Governing Intellectual Property Rights :

(i) Copyright Offences

- — 17 U.S.C. 506, Criminal Offences
- — 18 U.S.C. 2319, Criminal infringement of a copyright.
- — 18 U.S.C. 2318, trafficking in counterfeit label for phone records, copies of computer programmes or, computer programme documentation or packaging, and copies of motion pictures or other

audio-visual works, and trafficking in counterfeit computer programme documentation or packaging.

(ii) Copyright Management Offences
- 17 U.S.C. 1201, Circumvention of copyright protection system
- 17 U.S.C. 1202, Integrity of copyright management information.
- 17 U.S.C. 1203, Civil remedies.
- 17 U.S.C. 1204, Criminal offences and penalties.
- 17 U.S.C. 1205, Savings clause.

(iii) Trademark Offences
- 18 U.S.C. 2320, Trafficing in counterfeit goods or services.

(iv) Bootlegging Offences
- 18 U.S.C. 2319 A, Unauthorised fixation of and trafficking in sound recordings and music operators.

(v) Trade Secret Offences
- 18 U.S.C., 1831, Economic espionage.
- 18 U.S.C., 1832, Theft of trade secrets.
- 18 U.S.C., 1833, Exception to prohibitions.
- 18 U.S.C., 1834, Criminal forfeiture.
- 18 U.S.C., 1835, Orders to preserve confidentiality.
- 18 U.S.C., 1836, Civil procedure to enjoin violations.
- 18 U.S.C., 1837, Applicability to conduct outside the United States.
- 18 U.S.C., 1838, Construction with other laws.
- 18 U.S.C., 1839, Definitions.

(vi) Offences Concerning the Integrity of IP Systems
- 17 U.S.C., 506 (c.d.), Fraudulent Copyright Notice; Fraudulent Removal of Copyright Notice.
- 17 U.S.C., 506 (e), False Representation.
- 18 U.S.C., 497, Letters Patent.
- 35 U.S.C., 292, False marketing.

(vii) Offences Concerning the Misuse of Dissemination System :

— 18 U.S.C., 1341, Frauds and swindles.

— 18 U.S.C., 1343, Fraud by wire, radio or television.

— 47 U.S.C., 553, Unauthorised reception of cable service.

— 47 U.S.C., 605, Unauthorised publication or use of communications.

(c) *Cyber Stalking*

— 18 U.S.C. S 875, Interstate communications.

— 18 U.S.C. S 2261 A, Interstate stalking.

— 47 U.S.C. S 223, obscene of harassing telephone calls in the Columbia district in interstate or foreign communication.

(d) *Search and Seizure of Computers*

— 18 U.S.C. S 2510, et seq. Interception of wise, oral and electronic communications.

— 18 U.S.C. S 2710, et seq. Preservation and disclosure of stored wire and electronic communications.

— 18 U.S.C. S 3121, et. seq. Recording of dialing, routing, addressing and signaling information.

— 42 U.S.C. S 2000 aa, Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offences.

(e) *Guidelines Concerning Sentence Relevant to Cyber Crime*:

— IP Sentencing Guidelines.

— Sentencing Guidelines that apply to computer hacking offences.

— U.S. Sentencing Commission's Amendments to the Guidelines that relates to Computer Intrusions (w.e.f. Nov. 1, 2003).

U.S.A. has successfully enacted a lot of provisions relating to offences, their investigation and sentening. The country is leading in the field of checking cyber crime alone through efficient police forces, particularly F.B.I., and peoples cooperation. The number of cyber criminality also greater in the country on account of predominance of Internet and cyber technology in day-to-day life.

• *United Kingdom (U.K.)*

The United Kingdom has passed various legislations to deal with cyber crimes and to regulate the transactions on cyber space. The most important are *The Computer Misuse Act, 1990* and *'Regulation of Investigatory Powers Act, 2000.*

The Computer Misuse Act, 1990 has several substantive provisions concerning cyber offences and prescribes punishment for these offences. The said Act covers various offences which includes unauthorised access to computer materials, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised modification or alteration of computer materials.

The Act widens the scope of jurisdiction and as such does not require the accused to have been in the home country or the impugned act taking place in the country. Any kind of significant link with domestic jurisdiction is adequate enough to attract the jurisdiction of British Court. The fact of British citizenship has been made immaterial for offences under the Act. To cover the offence of "Unauthorised access to computer material", the accused should be in home country concerned at the time when he caused the computer to perform the function, or any computer containing any programme or data accused intended to access in unauthorised way by doing that act which was in home country that time. In order to cover offence of unauthorised access with intent to commit or facilitate commission of further offences, the accused was in the home country concerned when he did the act, which caused the unauthorised modification, or the unauthorised modification took place in the home country concerned.

Regulation of Investigatory Powers Act, 2000 makes it unlawful to carry out any authorised intentional interception of communication and prescribes procedures for doing the same by authorised personnel. It also contains provisions for acquisition and disclosure of data relating to communications and for the carrying out of surveillance. The Act provides for interception either without warrant in certain situations and with warrant in other situations. The Act also provides the list of authorities who may validly apply for an interception warrant. It also provides some specifical and general provisions to ensure misuse of the intercepted data.

Part III of the Act contains certain provisions relating to investigation of electronic data protected by encryption. These provisions empower authorities to issue directions to a person who is in possession of any description key of some data that is required to be discripted in the interest of national security or for detection or prevention of a crime or in the interest of the country. It can be issued also to ensure effective exercise or proper performance by any public authority. The Act also contains provisions for a Tribunal constituted for the purpose of dealing with any complaints from any actions done in pursuance of the Act.

• ***Australia***

Australia has enacted the Cyber Crimes Act, 2001 with a view to amend the existing laws of land relating to computer offences. The Acts which were amended by Cyber Crimes Act, 2001 are : *Australian Security Intelligence Act Organisation Act, 1979; Crimes Act, 1914; Criminal Code Act, 1995; Education Services for Overseas Student Act, 2000* and *Telecommunications (Interception) Act 1997.* The Act of 2001 has repealed the Part VI A of the Crimes Act 1914 in order to add computer offences in its schedule. According to the provisions of the schedule, the term "access to data of a computer" means (i) the display of the data by the computer or any other output of the data from the computer; or (ii) the copying or moving the data to any other place in the computer or to a data storage device, or (iii) the execution of programme in case of programme. The Division 477 of the schedule prescribes the following punishment for computer offences :

	Offences	Punishment
(a)	Unauthorised access, modification or impairment with intent to commit a serious offence.	(a) Serious offences means an offences punishable by life imprisonment or for a period of 5 years or more.
(b)	Unauthorised modification of data to cause impairment.	(b) 10 years imprisonment.
(c)	Unauthorised impairment of electronic communication.	(c) 10 years imprisonment.

Division 478 describes the following acts as other computer offences and punishments accordingly :

	Offences	Punishments
(a)	Unauthorised access to or modification of restricted data.	(a) 2 years imprisonment.
(b)	Unauthorised impairment of a data of data held on computer disk, etc.	(b) 2 years imprisonment.
(c)	Producing, supplying or obtaining data with intent to commit a computer offence.	(c) 3 years imprisonment.

• ***Austria***

The Austria has enacted a Federal Act, namely, *The Privacy Act*, 2000, which contains comprehensive legislation in the field of protection of privacy in the cyber space. The Act lays emphasis on the point that every body shall have the right to secrecy for the personal data and has the right to protect the same. The Act contains provisions and prescribes the condition under which the personal data could be collected or automatically processed and sets out procedures for legitimate use and transmission of data.

The controller or processor of personal data has been entrusted under section 14 of the Act to ensure security of data. The Act also provides for establishment of a Data Protection Commission vested with powers of supervision over the data storage and transmission and also a Data Protection Council which will advise the Federal Government and the State Government on request in political affairs of data protection.

Part X of the Act contains the penal provisions for various acts and omissions :

	Offences	Penalty
(a)	Use of data with intention to make a profit or to cause Harm.	(a) Imprisonment up to one year.
(b)	International and illegal gain or access to a data application or maintains an obviously illegal means of access, or transmits data	(b) A fine up to 18890 Euro.

	intentionally in violation of the rules on confidentiality, (S. 46, S. 47)	
(c)	Collection, process and transmission of data without having fulfilled his obligation to notify U/s 17; Or, engaged in transborder data transmission or committing without the necessary permits of the Data Protection Commission (U/s 13 of the Act). Or, violation of obligation of disclosure and information according to sections 23, 14 and 25; Or grossly neglects the required data security measures according to sec. 14.	(c) A fine up to 9445 Euro.

The cyber laws of Austria, therefore, adequately lay emphasis on the point of protection of right of privacy, which obviously includes data relating to private and family life also.

• *Belgium*

The Belgium Parliament enacted new provisions in Criminal Code in November 2000 in order to make computer forgery, computer fraud and sabotage criminal offence.

The section 550 (b) of the Criminal Code specify the computer crimes as follows :

(a) Any person, who is unauthorised makes an access or maintains his access to a computer system, may be sentenced to a term of 3 months to 1 year imprisonment and to a fine of (Bfr 5,200-5 m) or to one of these sentences.

If the offence, specified as above, is committed with intention to defraud, the term may be more stringent ranging from 6 months to 2 years.

(b) Any person who intentionally defraud or cause harm with such intention and exceeds his power of access to a computer system, may be sentenced to a term of imprisonment of 6 months to 2 years and to a fine of (Bfr. 5,200-20 m) or to one of these sentences.

(c) Any person, who intentionally or unintentionally either accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way, whatsoever or makes any use whatsoever of a computer system, causes any damage to a computer system or data which is stored, processed, or transmitted by such a system, may be sentenced to a term of imprisonment ranging from 1 year to 3 years and to a fine of (Bfr. 5,200-10 m) or to one of these sentences.

(d) Any attempt to commit offences as specified in (a) and (b) is also deemed offence and attracts the same sentence.

(e) Any person, who intentionally defrauds or causes harm, seeks, assembles, supplies, diffuses or commercialises data which is stored, processed or transmitted by a computer system and by means of which the offices, as specified in (a) to (d) may be committed, may be sentenced to a term of 6 months to 3 years and to a fine of (Bfr. 5,200-20 m) or to one of these sentences.

(f) Any person who abates or incites one of the offences specified in (a) to (e) to be committed may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of (Bfr. 5,200-40 m) or to one of these sentences.

(g) Any persons, who is aware that data has been obtained by the commission of one of the offences specified in (a) to (c) holds, reveals or divulges to another person, or makes any use whatsoever of data thus obtained, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of (Bfr 5,200-20 m) or to one of these sentences.

• ***China***

The Peoples Republic of China (PRC) promulgated regulations on December 30, 1957 for the sake of protection, security and management of all computer information networks. These regulations lay more emphasis on the protection of national interests, state secrets, protection of information systems and privacy of the individuals. The Regulations, *inter alia*, contains following provisions :

(a) No individual or unit can use the internet to cause harm to the national security, disclose state secrets, harm the

interest of the state, of society or of a group, the legal rights of citizens, or to take part in criminal activities.

(b) No individual or unit can use the internet to create, replicate, retrieve or transmit the following kinds of information :

- Inciting to resist or breaking of law or constitution or the implementation of administrative regulations;
- Inciting to overthrow the government or the socialist system;
- Inciting division of the country and harm national unity;
- Inciting hatred or discrimination among the people or harm the unity of the nationalities;
- Creating rumours, making falsehoods or distorting the truth and order of society;
- Promoting feudal system, obscenity, gambling, violence, murder, etc.
- Inciting terrorism or other criminal activities, or causing insult to others or distorting truth to slander people;
- Injuring the repulation and esteem of state organs;
- Other unlawful activities against constitution, laws or administrative regulations.

(c) No individual or unit can be engaged in the following unlawful activities which may cause harm to the security of computer system or networks :

- Nobody can use computer networks or network resources without obtaining proper prior approval;
- Nobody can without prior approval or permission may change network functions or to add or delete information;
- Nobody without prior permission may add to, delete, or alter materials stored, processed or being transmitted through the network;
- Nobody may deliberately create or transmit viruses;
- Other unlawful activities which harm the computer networks are also prohibited.

(d) The protection of privacy and freedom of computer network users has been ensured by the law. No individual or unit may, therefore, use the internet to violate the freedom and privacy of network users in violation of these regulations.

The regulation provides that the public security organisation may give warning and if anybody is found to be engaged in any kind of illegal activities and have illegal earnings, such earning may be confiscated by the appropriate authority. A fine up to 5000 RMB to individuals and 15,000 RMB to work units may also be imposed. For serious offences, authorities may close down the computer networks for six months and, if necessary, the public security can ask for cancellation of networks registration or business operating licence.

According to Article 21 of the Regulation, an establishment not implementing security techniques and protection measures and not imparting security education to networks users, etc., the public security organisation may give warning, take remedial action and may confiscate illegal incomes, if any, incoming from illegal activities. The Article 11 or Article 12 of Regulations contain provisions regarding registration of connecting network units and establishing proper account registration system and for fulfillment of the responsibility or registering users. If the violation continues despite warnings by the public security, the operation of network may be suspended for six months. Other forms of violations are governed by other relevant provisions of relevant laws and regulations.

• ***Estonia***

Criminal Code of Estonia contains the following sections that are specific provisions for prevention of the cyber crimes :

— S. 269 : Destruction or alteration of programmes and data stored in a computer.
— S. 270 : Computer sabotage.
— S. 271 : Unauthorised use of computers, computer system and networks.
— S. 272 : Interfacing or damaging the connections of computer networks.
— S. 273 : Spreading of computer viruses.

• *Germany*

German Penal Code contains several provisions governing cyber crimes and abuse of computer networks. Some of the relevant provisions are as follows :

— Section 202 a : Data Espionage.
— Section 263 a : Computer fraud.
— Section 269 : Fraud or falsification of legally relevant data.
— Section 270 : Deception or cheating in legal relations through data processing.
— Section 303 a : Alteration of data.
— Section 303 b : Computer sabotage.

• *Ireland*

Ireland has enacted a specific law, besides amendments in the existing Penal Code, namely, *'Criminal Damage Act, 1991'* to deal with damages caused to or by a computer system or network. According to section 1 (i) (b) of the Act, the term "data" means the "information in a form in which it can be accessed by means of a computer and includes a programme".

The term "damage", in relation to a data, means an action (i) to add to, alter, corrupt, erase or move to another storage medium or to a different location in the storage medium in which they are kept (whether or not property other than data is damaged thereby), or (ii) to do any act that contributes towards causing such addition, alteration, corruption, erasure or movement.

The section 2 (i) of the Act provides that a person who, without any lawful excuse, damages any property belonging to another with intention to damage any such property or being reckless as to whether any such property would be damaged, shall be deemed guilty of an offence. The sub-section (5) contains the provisions of penalty and according to that a person guilty of an offence under the said section shall be liable to summery conviction, resulting conviction of a fine not exceeding £ 1,000 or imprisonment for a term not exceeding 12 months or both, and in case of arson, the fine and imprisonment for life or both. When a person is found guilty of any other offence under this section, a fine up to £ 10,000 or imprisonment for a term not exceeding 10 years or both, may be imposed.

The offence of "unauthorised access to a data" has been defined in section 5 of the Act in the following words :

(1) A person who without a lawful excuse operates a computer :

(a) within the state with intent to access any data kept either within or outside the state, or

(b) outside the state with intent to access any data kept within the state;

shall, whether or not he access any data, be guilty of an offence and shall be liable of summary conviction to a fine not exceeding £ 50 or imprisonment for a term not exceeding 3 months or both.

(2) Sub-section (1) applies whether or not the person intended to access any particular data or any particular category of data kept by any particular person.

The section 7 (1) of the Act provides for criminal proceeding for offences committed by a person outside the state in relation to data kept within state or such other property. Section 7 (3) provides that a person charged with an offence under section 2 concerning data or an attempt to commit such offence may, if the evidence does not warrant a conviction for offence chared but warrants a conviction for an offence under section 5, be found guilty of that offence.

• ***Malaysia***

Malaysia has enacted a law, namely, *Computer Crimes Act, 1997* to deal exclusively with computer crimes. Under Part II of the Act, the following activities have been defined as offences :

(a) To perform a function on computer with intent to have an access to any programme or data held in any computer. Such access should be unauthorised and it is not necessary that the intent be directed towards any particular programme. The offender may be punished by a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

(b) If the above mentioned offences has been carried out with intent to commit an offence involving fraud or dishonesty or which causes injury as defined in the

penal code; It to abate or facilitate the commission of such offence whether by himself or by any other person, he shall be liable to get a fine not exceeding one hundred fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

(c) If a person does an act which he knows will cause unauthorised alteration of the contents of any computer, he will be liable to conviction of such offence. The penalty may be a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or both be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is committed with the intention of causing injury as defined under the Penal Code.

(d) If a person communicates directly or indirectly a number or code or password or other any other means of access to the computer of any person other than a person to whom he is duly authorised to communicate, such person on conviction is liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or both.

(e) A person having custody or control of any programme, data or other information which is held in any computer or retrieved from any computer which is not authorised to have in his custody or control shall be deemed guilty of an unauthorised access to such programme, data or information unless the contrary is proved.

The Act contains detailed provisions of jurisdiction and extradition of offenders in relation to these provisions. According to the law, offender has to be prosecuted irrespective of the fact of his nationality or citizenship and the offences committed by a foreign citizen has to be dealt with in respect of such offenses as if it has been committed within the territory of Malaysia.

- ***Malta***

The Electronic Commerce Act, 2001 is the specific enactment of Malta governing electronic commerce and connected matters. The Part VII of the Act contains amending provisions with regard to 'computer misuse' to be incorporated into the criminal code of the

country. The Act contains provisions for extra-territorial application of its penal sections and according to it if any act is committed outside Malta but it affects any computer, software, data or supporting documentation which is situated in Malta or is somehow linked or connected to a computer in the country, such act shall be deemed to be committed in Malta. The Extradition Act has also been amended for permitting extradition of cyber criminals and to tackle with an offence against the law relating to the computer abuse.

• ***Mauritius***

Mauritius has enacted various amendments to deal with computer related crimes. The country has enacted *'The Information Technology (Miscellaneous Provision) Act, 1998'* and various relevant provisions in the Penal Code. It has enacted the *'Economic Crime and Anti-money Laundering Act, 2000,* to deal specifically with money laundering. The Act contains specific provisions governing the prevention of money laundering through monitoring and reporting of suspicious transactions. It also provides provisions relating to international cooperation, mutual assistance with foreign countries and extradition of offenders. The country, therefore, has adequate law in the direction of prevention of cyber crimes and money laundering.

• ***Philippines***

'The Electronic Commerce Act, 2000' of Philippines contains provisions for the recognition and the use of electronic commercial and non-commercial transaction and documents and also penalties for unlawful application thereof and such other purposes. Section 33 of the Act makes the following activities as offences and prescribes punishment for them :

(a) Cracking or hacking through unauthorised access.
(b) Infringement of intellectual property rights.
(c) Violation of the Consumer Act and other relevant provisions of law by or using electronic data messages or electronic documents.
(d) Any other action violating the provisions of the Electronic Commerce Act, 2000.

• ***Romania***

Romania has made the following three enactments for prevention of cyber crimes and abuse of computer :

(a) Anti-corruption Law (Title III);
(b) Law No. 676 on 'The Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector; and
(c) Law No. 196/2003 on Prevention and Fighting of Pornography.

The Title III (Chapter II) of anti-corruption law prescribes provisions for prevention of cyber crimes and defines offences and their penalties. Section 1 of the Act contains provisions for offences against the confidentiality and integrity of data and computer system. Section 2 of the Act prescribes penalty for 'computer related offence' and the Section 3 contains provisions against child pornography through computer system.

Romanian law have the specific provisions guaranting the right to protection of privacy with regard to the processing of personal data in the telecommunication sector. It provides also for setting up a regulatory authority in order to ensure the minimum-security requirement to be adopted as preventive measures to ensure confidentiality and protect privacy and personal data.

Article B of law No. 196/2003 on Prevention and Fighting of pornography forbids the creation and propagation of paedophilic, zoophilic and necrophilic activities. The National Regulatory Authority on Communication (ANRC) may receive the complains against violation of cyber rules and in appropriate cases may require the internet service providers to block the access to the respective sites.

• *Singapore*

Singapore have enacted the *Computer Misuse Act, 1998* to deal exclusively with cyber crimes. The Act contains stiff provisions for "unauthorised access to computer materials with intent to commit or facilitate commission or an offence, "unauthorised modification, use of interception of computer materials", "obstruction of use of computer", "unauthorised disclosure of access code" and similar other offences.

A hacker committing the above mentioned crimes may be punished with fine not exceeding $100,000 or imprisonment for a term not exceeding 20 years or both. Even an attempt of abetment or attempts to commit any of the aforesaid offences are also liable

for the same punishment and actual happening of the offence is immaterial and irrelevant for the purpose. The Act provides wide range of powers to the police officer investigating a cyber crime including the power to inspect information contained in any computer and ordering anyone to provide encrypted information in his possession. The exercise of such powers, however, is subject to the written permission from Commissioner of Police and also consent of public prosecutor in certain matters. Police may arrest any person with or without warrant, if it has reasonable suspicion of committing an offence.

7

Cyber Crimes and Indian Response

Synopsis

7.1. Introductory Note

India has emerged as world's leader in the field of information technology. The earings from software export and IT services is now contributing substantially to the Indian economy. It is estimated that IT and ITES export will account for more than 35% of all foreign exchange income of India by 2003 and the IT industry will contribute to the 25% of incremental GDP growth between 2002 to 2008.[1] The number of internet subscribers in India is expected to increase up to 35 million by the end of 2005. The number of computer and IT literates is bound to increase leaps and bounds due to introduction of computer courses into the schools, colleges and university curriculums and various private computer institutes coming into existence at Block level.

With increase in the growth and development of information technology and cyber world, the possibility of increase in the crimes relating to computers has also increased simultaneously. Legislative step for regulating the electronic commerce and checking the cyber crimes have also become essential. The Indian Parliament therefore enacted the *Indian Information Technology Act, 2000* for combating cyber problems. The Indian response in the form of legislative actions as well as the IT revolutions is mainly limited to this Act and Rules and Regulations made thereunder.

7.2. The Indian Information Technology Act, 2000

Indian Parliament has enacted *'The Information Technology Act, 2000'* to provide recognition for transaction carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce" which involve the use of alternatives to the paper based means of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the India Penal Code, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for other matters connected therewith or incidental thereto. The important objective of the Act, of course, is to facilitate legal recognition and regulation of commercial activities through electronic medium.

7.3. Preamble and Coverage

The General Assembly of the United Nations by resolution No. A/GES/51/162; dated : 30th January, 1997 has adopted the Model Law of Electronic Commerce adopted by the United Nations Commission on International Trade Law. The said resolution recommends, *inter alia,* that all states should give favourable consideration to the said Model Law when they enact on revise their laws in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. The Indian Act is based mainly on the said UN resolution as well as on the UNICITRAL Model Law on Electronic Commerce.[2]

The Indian Act is based on the model law and governs mainly the e-commerce. The Act does not focus its attention towards the various forms of cyber crimes. The major issue covered under the provisions of the Act are as follows :

(a) Establish rules which recognise and validate contracts executed through electronic mediums;
(b) Covers default rules for contract creation and governance of e-contracts performances;
(c) Provides the definition and characteristic of a valid electronic writing and an original document;
(d) Contains provisions for the recognition of electronic signatures for legal and commercial purposes;
(e) Recognises the admission of computer evidences in courts and arbitration proceedings.

The law has been created because digital technologies and new communication systems have made dramatic changes in our lives. The business transaction now are increasingly being made with the help of computer and internet. The common masses and business community are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. The information stored in electronic form is not only cheaper but easier to store, retrieve and speedier to communicate. People were aware about these advantages but they were still reluctant to conduct business and transactions in the electronic form because there was lack of legal framework. Traditionally many legal provisions recognised only paper passed

records and document bearing signatures. There was an urgent need for legal changes to facilitate e-commerce because electronic commerce was likely to eliminate the paper based transactions. In order to meet such pressing need, the United Nations Commission on International Trade Law adopted on Model Law on Electronic Commerce in the year 1996. India being signatory to it, introduced 'The Information and Technology Bill, 1999' in the Parliament with view to facilitate Electronic Governance and to facilitate e-commerce in the country by way of suitable amendments in the existing laws of the country.

The statement and reasons of the Act states about the objectives of the Act. New communication systems and digital technology have made dramatic changes in the way we live. A resolution is occurring in the way people transact business. Business and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principle hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements as to writings and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents and records should bear signatures. The Law of Evidence is traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper based transactions, hence to facilitate e-commerce, the need for legal changes have become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

The preamble to the Act further says, "There is need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures. The will enable the conclusion of contracts and the creation of rights and obligation through the electronic medium.

It is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislation."

It further states, "It is also proposed to make consequential amendments in the Indian Penal Code and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions. It is also proposed to amend the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks and the Bankers Book Evidence Act, 1891 to give legal sanctity for books of account maintained in the electronic form by the banks." The above averments clearly show that the coverage of the act is limited to facilitating e-commerce and e-governance and does not include combating of cyber crimes of various forms.

7.4. Nature of Offences and Penalties

Although the objective of the Act is mainly to facilitate e-commerce and not specifically to govern cyber crimes, the Act, however, defines certain offences and penalties that deal with acts and commissions coming under the purview of the term cyber crimes. Chapter XI of the Act deals with offences and Chapter IX deals with penalties and adjudication. Chapter IX focuses on the following features :

(a) Regulating conduct in its unique way;
(b) Civil regulations to be employed by premise rather than criminal;
(c) The process of adjudication is entrusted to adjudicating officers rather than regular civil courts;
(d) Such adjudicating officers are required to know the law and IT or must have judicial experience;
(e) Adjudicating officers are vested with power of civil court;
(f) The proceedings to be conducted by such adjudicating officers are to be construed as judicial proceedings;
(g) The quantum of compensation to be calculated at market rate for loss or sufferings.

- ***Penalty for Damage of Computer, Computer System or Network***

Section 43 of the Act stipulates a liability to pay damages in the form of compensation not exceeding Rs. one crore to the persons so affected where any person without permission of the

owner or any other person, who is in-charge of a computer, computer system or computer network, does any of the following acts :

(a) accesses or secures access to such computer, computer system or computer network;
(b) downloads, copies or extracts any data, computer data base or information from such computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data base or any other programmes residing in such computer, computer system or network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes denial of access to any person authorised to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.

The explanations incorporated in the section for interpretation of its provisions are as follows :

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

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

(iii) "Computer virus" means any computer instruction, information data or programme, that destroys, damages, degrades or adversely affects the performance of a computer resources or attaches itself to another computer resources and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

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

The above definition is wide enough to cover almost all the cyber crimes in which computer system or network is involved. The section empower victims to claim compensation from offender.

• ***Penalty for Failure of Return, Information, etc.***

Section 44 of the Act prescribes certain legal formalities and states that if any person who is required under this Act or any rules or regulations made thereunder to furnish returns, maintain books, accounts, etc. The said provisions are :

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

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

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

• *Residuary Penalty*

Section 45 of the Act provides that whoever contravenes any rules or regulations much under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.[3]

According to the provisions contained in sections 46 and 47 of the Act, only an Adjudicating Officer appointed under the Act can adjudicate on these penalties or compensation on the basis of the following factors taken into consideration[4] :

(a) The amount of unfair advantage, as and when quantified, made as a result of the default;
(b) The amount of loss caused to any person as a result of the default;
(c) The repetitive nature of the default.

• *Offence Relating to Tampering with Computer Source Documents*

Chapter XI of the Act defines certain offences and prescribes the punishments for such offences. Section 65 defines the offences of tampering with computer source documents in the following words :

> "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 or computer network, when the computer code is required to be kept or maintained by the time being in force shall be punishable with imprisonment up to three years, or with fine which may be extended up to two lakh rupees, or both."[5]

For the purpose of explanation of this section, the word "Computer Source Code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.

• *Offence of Hacking*

Section 66 defines the offence of hacking with computer system. Under the provisions of this section, whoever with intent

to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking and whoever commits hacking shall be punished with imprisonment up to three years, with fine, which may be extended up to two lakh rupees, or with both.

There is, however, some difficulties between the offence of hacking as defined in section 66 and another defined in section 43 of the Act. In the case of former, the knowledge and intention is necessary to constitute the offence whereas in the later form of offence, no such *mens rea* is necessary to constitute an offence. Section 43 strictly restricts the unauthorised access to computer materials. Section 66 attracts offence when such access is made with the intent to cause, or with the knowledge that he is likely to cause loss or damage by an action.

Section 70 of the Act restrict similar type of access. Government is empowered by the section to declare any computer, computer system or computer network to be protected system, by publishing a notification in the Official Gazette. The Government may further pass an order in writing and authorise the person who may access to such protected systems. If any person or persons secures or attempts to secure access to such protected system without the authority from the Government he shall be according to section 70 (3) of the Act, punished with imprisonment of either description for a term which may extend to ten years and shall be liable to time. The section does not provide any upper limit of the fine that can be imposed for the offence of unauthorised access to a computer system. According to the provisions of the section, even an attempt is treated as an offence with equal gravity. These provisions intent to check the case of computer espionage and such other offences made against the protected systems and sesitive data.

- ***Offence of Obscene Publication in Electronic Form***

Section 67 of the Act makes the publication of information which is obscene in electronic form an offence. According to this provisions, whoever publishes or transmits or causes to be published in the electronic form, any material which is lascious or appeals to the prurient interest or 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. The section covers the cyber crimes such as child pornography existing in the cyber space.

• *Offence of Non-compliance of Instructions from Controller*

The Controller of Certifying Authorities are appointed by the central government under the provisions of section 17 of the Act. Under section 68 of the Act, the Controller is empowered to direct a certifying authority, or any employee of such authority by order to take steps or cease carrying out of such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules and any regulation made thereunder. Any person failing to comply with such order shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or both.

Sub-section (1) of section 69 of the Act empowers the Controller to issue direction to any agency of the Government to intercept any information transmitted through any computer resource, where he thinks it expedient or necessary so to do in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign countries or public order or for preventing incitement to the commission of any cognizable offence. The Controller, however, has to assign reasons while giving such a direction to any agency.

The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been defined under sub-section (1) of section 69, extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred to in section 69 (2) shall be punished with an imprisonment for a term which may be extended to seven years.

- *Offence of Misrepresentation or Suppression of Facts*

According to section 71 of the Act[6], whoever makes any misrepresentation to, or suppression of any material fact from the Controller or the Certifying Authority for obtaining any licence or digital signature certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees or with both.

- *Offence of Breach of Confidentiality and Privacy*

According to section 72 of the Act, save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees or with both.

- *Offence of Publishing Digital Certificate False in Certain Particulars*

Section 73 (1) provides that no person shall publish a Digital Signature Certificate or otherwise make it available to any person with the knowledge that the certifying authority listed in the certificate has not issued it; or the subscriber listed in the certificate has not accepted it; or the certificate has not been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

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

- *Offence of Publication for Fraudulent Purpose*

Section 74 of the Act stipulates that whoever knowingly creates, publishes or otherwise makes available a digital signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two

years, or with fine which may extend to one lakh rupees, or with both.

7.5. Miscellaneous and Subsidiary Provisions

Certain procedures and other miscellaneous provisions have been laid down in the Act which may be summed up as follows:

(a) Offences Committed Outside India : Section 75 provides that the application of the Act shall be extended beyond the territorial limits of India and shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality, if such act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

(b) Confiscation : Section 76 stipulates that any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made thereunder has been or is being contravened, liable to confiscation. This provision helps the enforcing agencies in collection of evidence and prevention of crime further.

(c) Penalties or Confiscation not to Interfere with other Punishments: Section 77 provides that no penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

(d) Power to Investigate Offences, Enter, Search, etc. : Section 78 of the "Act provides that, notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), only a police officer not below the rank of Deputy Superintendent of Police shall investigate an offence under the Act. The provision is mandatory and, therefore, any investigation done by a police officer below the rank of D.S.P. shall vitiate the investigation.

Section 80 of the Act further provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a state government authorised 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. The expression "public place" includes any public conveyance, any hotel, or any other place intended for use, or accessible to the public. Here the expression obviously excludes the power to enter and search the residential houses and other private places. Subject to these provisions, the provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall be made applicable to any entry, search or arrest.

(e) Offence by Companies : According to section 85 of the Act, where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be prosecuted against and punished accordingly, unless any such person liable to punishment proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Further, where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. For the purpose of explanation, the "company" means any body corporate and includes a firm or other association of individuals and "director", in relation to a firm, means a partner in the firm.

(f) Liability of Network Service Provider : Section 79 stipulates that no person providing any services as a network service provider shall be liable under this Act, rules or regulation made thereunder for any third party information or data made available him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. For the purpose of explanation to this section, the word "network service provider"

means an intermediary and "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

7.6. Certain Shortcomings

From the above discussion, we have come to know that the focus of Indian Information Technology Act was to cover the various aspects of e-commerce and not to check the cyber crimes. Although there are some definitions of contraventions and offences and their penalties and punishments have also been contained therein, yet many issues have been left unresolved. Many procedural aspects and ways of crime detection and prevention has not received proper attention of the law makers. These shortcomings may be discussed under the following heads :

(a) Power of Police to Enter and Search Limited to Higher Officers and to Public Places : The Act although gives wide powers to police officer not below the rank of Deputy Superintendent of Police (DSP), to enter and search the public places and arrest without warrant any person who is reasonably suspected of having committed or of committing or of being about to commit any offence under the Act, but such power is limited to the extent of "public places" only. Also such criminal offences may be committed or being committed, at large scale from residential houses and such other private places. The Act's provision that only an officer of the rank of DSP can investigate the case or make search and seizure is also a serious constraint because Police Departments do not have many DSP rank officers to tackle so many cases. Moreover, such type of blanket of power of search and seizure may also result into the violation of privacy and human rights.

(b) Inapplicability to Certain Laws and Documents : Sub-section (4) of section 1 of the Act stipulates that nothing in the Act shall apply to negotiable instruments (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881; a power of attorney as defined in section 1-A of the Power of Attorney Act, 1882; a trust as defined in section 3 of the Indian Trust Act, 1882; a will as defined in section 2 (h) of the Indian Succession Act, 1925 including any other testament; any contract for sale of immovable property or any kind of interest in such property; and any such kind of documents or transactions which may be notified

by the Central Government in the Official Gazette. Such type of wide range of inapplicability of the Act has substantially reduced its utility.

(c) Lacks Definition of Cyber Stalking and Harassment : Chapter XI of the Act, entitled "offences", deals with hacking, damage to computer source code, publishing of obscene information and breach of protected system. It, however, completely ignores cyber stalking and other form of harassment. Due to this drawback, for example, the accused of Delhi based, Ritu Kohli, the victim in the first ever case of cyber stalking reported in India, was booked under the relatively innocuous section 509 of the Indian Penal Code.[7]

(d) Improper Definition of Hacking : The definition of "hacking" given under section 66 (1) of the Act is not in conformity with the internationally acknowledged term. The scope of section 66 (1) is so wide that any activity of a person done over the internet may be covered under mischief of the section. Further, word "wrongful loss" has not been defined in the Act. Furthermore, there are no parameters prescribed to prove the diminishing value of information. Pawan Duggal, a cyber expert and advocate of Supreme Court of India, rightly says, "Internet is like a huge ocean, and the act wrongly makes the service provider liable for all third party data and information posted on it."[8] There is also no norms and standards for proving injury in the electronic medium and internet.

(e) Qualification of Adjudicating Offices not Prescribed : Section 46 of the Act provides for appointment of an officer not below the rank of a Director or an equivalent officer of state government to be an adjudicating officer for holding an enquiry under the Act. Sub-section (3) of section 46 stipulates that no person shall be appointed as an adjudicating officer unless he possesses such experience in the field of information technology and legal or judicial experience as may be prescribed by the Central Government. But Central Government has framed the specific requisite qualification for the purpose.

(f) Lacks of Steps for Checking Internet and Copyright Piracy: There is apparent act of appropriate measures in the field of checking the violation of copyright of music, songs, pictures, etc., in the Act, despite such infringements have become Sampant after

advent of internet. Such type of violation of intellectual property rights and piracy in the cyber space have several for reaching civil consequences.

(g) Lack of International Cooperation : The impact and area of operation of cyber crimes are global and therefore, any effort at the level of a particular country cannot be fruitful. It is not possible to check criminal acts committed through the internet by aliens residing and operating from another countries, unless there are concrete steps taken at international level through international cooperation. Such positive global cooperation is yet awaited.

(h) Lack of Appropriate Guidelines for Investigation : The traditional investigatory procedures are not capable enough to detect and collect evidences in the field of cyber crimes. The cyber space is under rapid development and law, therefore, must be amended properly to cope up with the same. Apart from amending the Indian Evidence Act, 1872 and the Bankers Book Evidence Act, 1891, there is need of adopting new techniques for making electronic records as a valid evidence in a court of law. The present methods adopted by Police are still under the rudimentary stage of development.

7.7. Future Prospects and Needs

The enactment of the Indian Information Technology Act, 2000 may be stated to be India's modest beginning in the field of cyber space. This initiative may be called appropriate and in time as India is now being recognised as one of the world leaders in the field of information technology. However, there is need to cover more and more cyber activities under the purview of the cyber laws. The problem may be solved by bringing necessary amendments in the Indian Penal Code as per changing facets of cyber crimes. There is need of legislative attention in the area of data protection also. Such legislative actions are necessary for the sake of protection of Indian computer and internet users including Indian organisations, companies, business firms and individuals along with their right to privacy.

Procedural aspects including investigation and appreciation of evidence has not appropriately been dealt out by the Indian Parliament. Section 76, 78 and 80 of the Act deals with the matters concerning investigation, seizure, search and arrest and also make

the provisions of Criminal Procedure Code applicable to such actions of entry, search and arrests made by the competent authorities. Some necessary amendments have also been made out in the Indian Penal Code and Indian Evidence Act in this direction. However, the challenges faced by the law enforcing agencies are still in existence because offenders are more equipped than the law enforcing agencies. A well-defined guidelines with the regard to surveillance, search and seizure, forensic aspects, evidence collection in transnational cases, etc., is the need of the present day.

The criminal activities in the cyber space are not limited to the level of any particular territorial limits. Any isolated efforts at national level cannot be effective in controlling the cyber crimes. It is, therefore, essential to take proper steps toward establishing the international cooperation in area of combating the cyber crimes as envisaged in Article 35 of the Council of Europe Convention on Cyber Crimes. Method and mechanism as suggested by Council of Europe Convention may be adopted for coordinating with international agencies in the field of collection of traffic data[9], interception of content data[10], preservation of stored data[11], search and seizure of computer data[12], etc.

Special courts should be set up for the trial of cyber crimes and its presiding judges should be properly and technically trained to evaluate evidence technologically. Efforts should be made for creating awareness among general public and capability building among the members of law enforcing agencies and criminal justice administration. Adequate number of technically competent investigating officers and forensic experts should be employed in the police department and a separate cell should be set up to deal with the cyber crimes effectively.

Table 7.1

Penal Provisions in Indian IT Act, 2000

Sl. No.	Section	Penal Provision	Maximum Penalties
1.	Sec. 53	Penalty for damage to computer, computer system and computer network	Rs. one crore
2.	Sec. 44 (a)	Failure to furnish any	Rs. 1,50,000

		document, return or report to the certifying authority	
3.	Sec. 44 (b)	Failure to file any returns or furnish any information, books or other documents	Rs. 5,000
4.	Sec. 44 (c)	Failure to maintain books of account or record	Rs. 10,000
5.	Sec. 45	Contravention of any rule or regulation for which no penalty is provided separately	Rs. 25,000
6.	Sec. 65	Tampering with computer source documents	Up to three years imprisonment and fine up to Rs. 2 lakh or both
7.	Sec. 66	Hacking with computer system	Up to three years imprisonment and fine up to Rs. 2 lakh or both
8.	Sec. 67	Publishing of information which is obscence in electronic form	Up to Rs. 2 lakh or both
9.	Sec. 72	Breach of confidentiality and privacy	Up to 2 years imprisonment and fine up to Rs. 1 lakh
10.	Sec. 73	Publishing digital signature certificate false in particulars	Up to two years imprisonment and fine up to Rs. 1 lakh

References

1. Nasscom-Mckinsey Study, 2002, www.nass.com.org
2. UNICITRAL Model Law of Electronic Commerce, 1996. Adopted by UN General Assembly vide Resolution No. A/Res/51/162 : dated : 30 January, 1997, www.un.or.at/uncitral/text/electcolm/m/-PS.
3. Sec. 45, of the Information Technology Act, 2000.
4. Sec. 46 and 47 of the Information Technology Act, 2000.

5. Section 65, The Indian Information Technology Act, 2000.
6. Section 71, The Indian Information Technology Act, 2000.
7. *The Times of India*, Patna, 30 December, 2004.
8. *Ibid.*
9. Article 33 of the Council of European Convention on Cyber Crimes.
10. Article 34, *Ibid.*
11. Article 16, *Ibid.*
12. Article 19, *Ibid.*

8

Mens Rea and Criminal Liability

Synopsis

8.1. Introduction

• *Crime : Definition*

Usually crime is defined as an intentional act or omission in violation of a criminal law (statutory and case-law), committed without any proper defence or justification and prohibited by the state. The word crime, as held by Supreme Court, may also be defined as the commission of an act specifically forbidden by the law and it may be an offence against morality or social order, which subjects to doer to legal punishment.[1]

• *Conditions of Crime*

The following conditions or facts must exist for awarding punishment to a criminal who has been alleged to commit an act punishable by the law :

(i) The accused must be of competent age, irrespective of his act;

(ii) Criminal act must be voluntary and engagement in such act should be without compulsion;

(iii) The accused must have a criminal intent;

(iv) To constitute a crime, an act must be classed legally an injury to the state and not merely as a private injury, or tort.

Thus, it is obvious from the above mentioned conditions of crime that mere keeping an intention to commit a crime does not constitute a crime unless such intention is following by an act resulting in injury to the state or individual.

• *Elements of Crime*

Moreover, the crime in general consists of two elements :

(i) the criminal act or omission; and

(ii) the mental element.

Such requirement of mental element, generally called as the guilty mind, is referred to in legal terminology as "Mens Rea". According to the mens rea concept, the law seldom holds a person accountable or guilty if he has acted unconsciously or involuntarily or has been so completely without control of his mind or physical

---

[1]T.K. Gopal-Vs-State of Karnataka = AIR 2000 SC. 1669 = 2000(2) crimes 245 (sc).

faculties that he could not have formed a criminal intention. The following circumstances negate the intent even though the capacity to perform an act exists :

(i) insanity,
(ii) accident,
(iii) ignorance or mistake of fact,
(iv) age,
(v) self-defence,
(vi) duress, and
(vii) coercion.

"Motive" is an essential element of crime, which is distinguishable from the "Intent". "Motive" is a "reason" or a "moving cause", whereas the "Intent" is "purpose" or "resolve" to do an act. Motive, of course, is often important while offering proof of existence of the essential element of the crime. The "act" of the accused and the "intent' must be concurrent to constitute an occurence of offence or a crime. This relationship exists when the act of the accused is in the proximity of the injury involved.

An "act" becomes an offence or a crime when it is so defined by statutory enactment or common law. Thus, an act or behaviour that was permissible at one time may, at a later time, be declared as an "illegal" act. There are many acts which are publicaly considered deviant, abnormal or abhorrant but that are not crimes, while some acts are defined by law as crimes but are not popularly considered as wrong or abnormal. The importance of mens rea (guilty mind) is reflected from the legal maxim—*"Act is non facit reum nisi means sit real"*; i.e., the act does not constitute guilt, without the guilty mind.

The doctrine of *nullum crimen sine lege* (no crime without a law) still holds good in law. There can be no crime without a statute that quite specifically forbids the behaviour involved. The doctrine *no ex post fact* (retrospective) legislation still exists and, therefore, no person can be punished at later date for a behaviour or act that was not criminal when committed. Every person is presumed to have some knowledge of the law. An individual is held accountable for violations, as per concurrent law and system of justice irrespective of the fact whether or not he is familiar with the statues.

The definition of crime given by noted scholars are as follows:

(i) A crime is an act committed or omitted in violation of a public law either forbidding or commanding.
(William Blackstone : *Commentaries;* Vol. IV, p. 5).

(ii) Crime is an intentional act or omission in violation of criminal law committed without defence or excuse, and penalised by the state as a felony or misdemeanour.
(Tapan : *Who is Criminal*)

(iii) A wrong regarded as the subject matter of criminal proceeding is termed a criminal wrong or a crime.
(Salmand : *Studies in Jurisprudence and Criminal Theory,* p. 10)

(iv) Crime is a wrong as whose sanction is punitive, and is no way remissible by any private person but is remissible by the crown, if remissible at all, is again not only procedural but also is incomplete in so far as it leaves out of its purview the offences compounable by the person who has been injured even without any interference by the crown or state.
(Kenny : *Outlines of Criminal Law,* 1952, App-I)

(v) Crime is an act that has been shown to be actually harmful to the society, or that is believed to be socially harmful by a group of people that has power to enforce its beliefs and that places such act under the ban of positive penalties. Thus, a crime may be regarded as an offence against the law of the land.
(Gillin, J.L., Criminology & Penology, 3rd, p. 6)

(vi) Crimes are acts forbidden by the law under pain of punishment. (Srephen : *"A General View of the Criminal Law of England"*, (1), 1863)

To sum, we may say that crime is an act of transgression against the public order rather than against moral or private orders.

• ***Criminal Liability : Definition and Scope***

A person is not guiltly of an offence unless his liability is based on conduct which includes a voluntary act or the omission to perform an act of which he is physically capable. Liability for the commission of an offence may not be based on an omission unaccompanied by action unless the omission is expressly made

sufficient by the law defining the offence, or a duty to perform the omitted act is otherwise imposed by law. Criminal liability for omission is exceptional. Many statutes make it an offence to omit to do something. Nevertheless, liability for omission, though exceptional, is not limited to crimes expressly defined by statute as omission offences.

The law distinguishes between negligence which originates a civil liability and the one on which a criminal prosecution can be founded. In criminal cases there must be mens rea or guilty mind. In the matter of rashness or guilty mind of a degree, which can be described as criminal negligence, mere carelessness is not enough.[2] The word "civil nature" is wider than the word "civil proceeding", the object of civil proceedings is the recovery of money or other property or the enforcement of a right but the object of criminal proceedings is the punishment of a public offence.[3] If the dispute is purely of civil nature, the courts cannot allow the parties to get the dispute settled in a criminal court.[4] However, a case of breach of trust is both civil wrong and a criminal offence. There would be certain situation where it would be predominantly be a civil wrong and may or may not amount to a criminal offence.[5] There is no bar to allow continuance of civil and criminal proceedings simultaneously but, however, criminal proceedings should be given preference.[6]

In the matter of user of forged documents as genuine, the criminal liability cannot be established merely on the ground that the accused is benefited from the said forgery and fraud, unless his connection or complicity with the offences is at least *prima facie* indirected from the complaint or investigation reports. The term "strict liability" or "absolute liability" mean that criminal liability of a person established by his active conduct, which appears to be the visible cause of injury or harm without inquiry into the state of mind at the time of act. The guilty mind need not to be proved in a crime like hacking. The burden of proof shifts from prosecution to defendant and prosecution has to prove only alleged actor omission.

8.2. Historical Perspectives

The growth and development of criminal law went ahead hand in hand with the growing requirement of human beings and the social system as a whole. The contents of legal and

classical texts bears ample testimony to the pattern of its development. Dharmsutras, which are the earliest texts dealing with legal matters, contain no elaborate dicta on criminal law. Manusmriti laid the foundations of the restructured Hindu Society after the advent of Buddhism, and it is in this work that we find the special mention of certain issues pertaining to criminal law. These issues appear as a part of titles of law put forth in the Manusmriti. The development of criminal law in the era of the composition of Manusmriti seems significant. It was an era of deep transition in which Brahmanism was reasserting itself. The social situation of this transition must have caused widespread dislocation and the leaders of Brahmanical revival had therefore to prescribe strict laws for punishment of deviation.

But the height of sophistication of the traditional Indian system of criminal law was reached in the era of later Smritis, when the society attained a high degree of complexity as a result of growth of trade and industry. This is apparent by the elaborate treatment given to various kinds of crimes and the intricate provisions for dealing with them in the Smritis of Brhaspati, Narda, and Katyayana. These Smritis give detailed consideration to crimes against person, including abuse and assault of various kinds, crimes relating to property, both public and private, and sex offences. The provisions relating to all these types of crimes bear the impress of the prevailing social stratification. The system of law naturally sought to fortify and legitimate the basic structure of society. The nature and severity of the punishment prescribed for the same offence varied according to the varna of the person against whom it was committed. It also varied according to the varna of the offender.

Caste hierarchy played an important part in making of the legal code.[7] The heaviest punishments were prescribed for Shudras whereas Brahmanas were given immunity from heavy punishments. Gautama provides that if a Shudra criminally assaults twice-born persons, he shall be deprived of the limb with which he offends.[8] Manu and Yajnavalkya provide that one who breaks the skin of an equal caste person shall be fined hundred Panas,[9] if he cuts a muscle, six Niksakas; and for breaking a bone, banishment should be given.[10] It is remarkable that Narada considers adultry with female ascetic a grave crime, while

Yajnavalkya prescribes only a fine of twenty-four Panas for that offence.

Elaborate rules for receiving the facts of the dispute, categorisation of the title of law to which the dispute belongs, pleadings and examinations of the evidence, and pronouncement of judgement are given by the later Smritis. These are rules for the summoning of the defendent, exemption from appearance before the court, and appointment of someone else to represent one's case, adjournments, etc., are also laid down therein. Forgery of documents finds mention in texts as ancient as the Vishnu Dharmasutra and the Smritis of Manu and Yajnavalkaya. The merchant class seems to have acquired great importance in society during the period around second to sixth century A.D. Katyayana Smriti lays down that some merchants should be included in the court and they should listen to the courses and look to the administration of justice. With the decline of Indian maritime trade in later centuries, sophisticated legal provisions governing commerce and industry seem to have fallen into disuse. But the tradition of law did not lose all vigour. Legal commentaries and digests continued to be written at least up to nineteenth century. But the traditional judicial nations, such as those put forward by the Mitakasara and the Dayabhaga, have continued to guide the life of Indian people till contemporary time. The developments taking place in society due to advent of concurrent scientific developments of course compelled the legislation and legal enforcement agencies to bring necessary changes time to time in the law and its procedures.

The main task that came before a legal enforcement authority was to determine as to when a crime is said to have committed and when and for what actions a person is to be held liable for punishment. The notification of strict liability was prevalent in all societies and any person whose act appeared as the visible cause of the harm was held responsible for it. Even ancient Hindu laws also followed a similar system, though it recognised the civil and criminal branches of law but did not strictly adhere to the distinction between crimes and civil wrongs. Hindu law, therefore, laid stress on punishment even for those wrongs which modern law would consider purely civil. Modern law recognised a new concept known as mens rea and role played in a crime committed in order to determine criminal liability.

8.3. Mens Rea in Indian Criminal Law

Criminal law of India is mainly based on Indian Penal Code, which was originally drafted by Lord Macaulay and thoroughly revised by Sir Barnes Peacock. The Indian Penal Code is the sole authority of Indian although some of the statutes also contain certain incidental provisions relating to criminal liability. The maxim *'Actus non facit scum nisi means sit rea'* has no application to offences under the code.

The world 'mens' means 'mind'. Mens rea in the criminal law means the state of mind of the actor, or his intention. The mens rea is the necessary mental element of the crime. According an old legal axiom, "An act does not make the door of it guilty, unless the mind be guilty, "or" unless the intention be criminal". The intent and the act must both concur to constitute a major crime, thus, both the actus reus and means sea are necessary elements of a crime. Mens rea has thus been held to mean a guilty mind; a guilty or wrongful purpose; a criminal intent. Moreover, some definitions distinguish between the general and specific state of mind.

Mens rea is an integral part of a crime unless it is specifically or by implication excluded and therefore, a person is not guilty unless he is proved to have a guilty mind.[11] There are cases in which intention and knowledge are ingredients of the offences and have to be established either by evidence or legal inference.[12] The word "aid" and "abet" means to help, assist, or facilitate the commission of a crime, or to promote the accomplishment thereof, or to help in advancing or bringing it about, or to encourage, council, or incite as to its commission. The words "aid" and "abet" are not, however, synonymous, although both words are ingredient of "abetment". There is requirement of mens rea in abetment also and in order to constitute abetment, the abettor must be shown to have "intentionally" aided the commission of the crime. Mere proof that the crime charged could not have been committed without the inter position of the alleged abettor is not enough compliance with the requirement of sec. 107 IPC and involves active complicity on the part of the abettor at a point of time prior to the actual commission of the offence, and it is of the essence of the crime of abetment that the abettor should substantially assist the principal culprit towards the commission of the offence.

The expression mens rea is used to mean the mental state expressly or impliedly mentioned in the definition of crime charged. An act does not make a person guilty unless the mind is guilty. The 'mens rea' in criminal negligence was defined by Lord Diplock in the following way, "without having given any thought to the possibility of there being such risk or having recognised that there was some risk involved, had nevertheless gone on to take it". Section 265 IPC penalises the "fraudulent use of false weight or measures of capacity", which section 50 of the Standards of Weight and Measurement Act, 1976 (Act LX of 1976) penalises the use of any non-standard weights, measures. No mens rea is required for offence falling under sec. 50 of Act of 1976, which mens rea is the necessary ingredient of section 265 IPC. This simply because mere possession of a non-standard weight shall result in the commission of an offence in the case of former.

There is well known legal maximize, i.e., *'Actus non facit seum nisi mens sit rea'*, which means, the intent and the act must both concur to constitute the crime. Mere intention to commit an act defined as a crime is not punishable. For the offence of attempted murder punishable under section 307 of the Indian Penal Code, it is necessary for the prosecution to prove that the accused had one of the four special mens rea mentioned in section 300 of the Indian Penal Code which defines murder.

8.4. Mens Rea in English Criminal Law

The common law judges in England used to adhere to the maxim of mens rea for the sake of establishing criminal liability before emergence of penal laws in the country.[13] Thereafter a conflict arose between common law judges and the Parliament soon after emergence of legal legislations. Justice Cave observed in *Chrisholm Vs. Daulton*[14] case that "it is general principle of criminal law that there must be an essential ingredient in a criminal offence, some blame worthy condition of mind. Sometimes it is negligence, sometimes malice, sometimes guilty knowledge but as a general rule there must be something of that kind which is designed by the expression mens rea. Similarly, Justice Stephens also observed in Tolsoris[15] case that "the full knowledge of every crime contains expressly or by implication a proposition as to a state of mind. Therefore, if the mental element of any conduct

alleged to be a crime is proved to have been absent in any given case, the crime so defined is not committed".

However, the importance of mens rea were seen gradually being replaced by the introduction of strict liability in the field of judiciary of England. This tendency is apparently reflected from the following observations in *'Brend Vs. Wood'*[16] which states that "It is of the utmost importance for the protection of the liberty of the subject that a court should always bear in mind, that, unless a statute either clearly or by way of necessary implication rules out mens rea as a constituent part of crime the court should not find a man guilty of an offence against the criminal law unless he has a guilty mind."

As regards an absolute offence committed, J. Aderson B. has held in *A.G. Vs Lockwood*.[17] "The rule of law, I take it, upon the construction of all statutes, and therefore applicable to the construction of this, is whether they be penal or remedial, to construe them according to the plain literal and grammatical meaning of the words in which they are expressed unless that construction leads to a plain and clear contradiction of the apparant purpose of the act or to some palpable and evident absurdity." There is no need to prove mens rea unless it would be a plain and clear contradiction of the apparant purpose of the Act to convict without proof of mens rea. But this assumption is not appropriate and acceptable by all. It is firmly established by many legal authorities that mens rea is an essential ingrediant of every offence unless some reason can be found for holding that it is not necessary. Simultaneously it is also established that the fact that other section of the Act expressly require mens rea to be proved, for example, because they contain the word "knowingly", is not by itself sufficient to justify a decision that a section which is silent as to mens rea creates an absolute offence. In order to establish the guilt, all relevant circumstances and intention of legislation has to be seen unless there is a clear indication in the Act that an offence is intended to be an absolute offence. It is also well established principle that if a penal provision is reasonably capable of two interpretations, that interpretation which is most favourable to the accused must be adopted.[18]

8.5. Abetment of Offence

The act "abetment" deals with the presence of those who aid or afford aid or facilitate the commission of an offence. The word is wide enough to mean and include—advocating, arousing, assisting, backing, contributing, cooperating with, encouraging, facilitating, goading, helping, inciting, nourishing, prompting, serving, stimulating, supplying aid, supporting, to maintain or patronise, to set on. The word "instigation" in the Concise Oxford Dictionary has been defined as "urge on, incite, bring about persuation" and in the Webster Dictionary, it has been defined as "urge forward, provoke with synonyms of stimulate, urge, spur, provide tempt, incite impel, encourage, animate".

In order to constitute abetment, the abettor must be shown to have "intentionally" aided the commission of the crime. According to section 107 IPC, the "abetment" comprises (i) instigation to do that thing which is an offence, (ii) engaging in any conspiracy for the doing of that thing, and (iii) intentionally aiding by an act or illegal omission. Section 108 of IPC defines an abettor as a person who abets an offence or who abets either the commission of an offence or the commission of an act which would be an offence.

The definition of abetment includes not merely instigation but also conspiracy and aiding.[19] Mere failure to prevent the commission of an offence is not an abetment, if there is nothing to show that the accused instigated the commission of offence.[20] In order to convict a person of the offence of abetment, it must be proved that he instigated the person committing the offence or that there was an agreement between them to commit the offence.[21] The existence of mens rea is necessary for abetment also. If the person who lends his support does not know or has no reason to believe that the act which he is aiding or supporting was in itself a criminal act, it cannot be said that he intentionally aids or facilitates the commission of an offence and that he is an abettor.[22] The dishonest concealment of fact with intention of causing wrongful gain to one person or wrongful loss to another person also come within the ambit of the abetment.

8.6. Criminal Liability and Role of Mens Rea in 'Indian Information Technology Act, 2000'

The offences defined and penalties in the Indian Information Technology Act, 2000 have been divided into two categories in

view of the broad area of criminalisation in the cyber space. The first category of violations, i.e., section 43, 44 and 45 of the Act, are not subject to criminalisation and mens rea is not made applicable to them. The second category of offences are concerning tampering with computer source documents (sec. 65), hacking with computer system (sec. 66), and publication of fraudulent purpose (sec. 74), and mens rea has been made integral part the allegation of offence by inducting words like "knowledge" or "intention" therein. There are some other acts or omissions, i.e., section 71 and 73 of the Act, that are having criminal liability under strict liability principles.

The recent case studies show certain lacuna in the IT laws of India. For example, the arrest of Bazee.com CEO Avinash Bajaj has put a spot light on the inadequacies of Indian Information Technology Act, who was arrested under section 67 of the Act for publishing obsence electronic content. Unlike the Indian Penal Code, section 79 of the Act puts the onus of proving innocence on the network service provider, including in the case of Bazee.com. But the section 79 of the IT Act says, "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party of data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had excercised all due diligence to prevent the commission of such offence or contravention".[23] The experts are of opinion that the term "due diligence" is open to misinterpretation by the police and needs clarification. According to the defence lawyers, the arrest of Bajaj was unjustified as Bazee.com had removed the offending MMS clip immediately after the transaction was completed and this immediate removal shows due diligence on the part of the portal and also rules out its prior knowledge about the MMS clip.

Furthermore, the experts raised their eyebrows on the court's denial of bail on the ground that the user agreement bore no signature of the main accused Ravi Raj, the student of IIT Kharagpur. This is a question concerning disallowing of electronic evidence under the IT Act and the revised Indian Evidence Act. At this rate, the experts further say, all e-commerce in India will be out-lawed for want of signature and the main accused may be

the Indian Railway online site, which transacts a monthly business of Rs. 18 crore for sale of 60 lakh tickets daily.

The case also draws attention towards the **Indecent Representation of Women (Prohibition) Act, 1986 (IRWP Act).** Section 3 of the IRWP Act prohibits all persons from getting involved, directly or indirectly, in the publication or exhibition of any advertisement containing indecent representation of women in any form. Section 7 of the IRWP Act fixes liability for indecent representation on the company and every person who was in charge of the conduct of the company's business.

There are two principal types of internet auctions conducted by auction websites : Business-to-consumer (B2C) auctions, and consumer-to-consumer (C2C) auctions. In the case of B2C auctions, the owner and operator of the internet auction website have a certain degree of control over the goods auctioned of their websites. However, in C2C auctions, C2C auction site has no control over the goods auctioned; it merely acts as a lender of virtual market place for buyers and sellers to strike their deals. In the case of B2C auctions, internet auction websites have knowledge of the goods sold, as they are in each case an actual party to such transactions. However, in C2C auctions, auctions sites have no such knowledge of the goods sold as they are not a party to such transactions.

An analysis of the offending sale reveals that Baazee was probably not an accused for the following reasons : the actual video clip was not shown on Bazee's website but instead the seller offered to e-mail the video clip to the buyers directly. Baazee was neither the owner nor in possession of the video clip. Baazee was not the buyer or seller of the video clip, Baazee was merely acting as an auction house space provider to the seller; and the sale violated Baazee's policy prohibiting the sale of pornographic content through its website. The element of "knowledge" which is essential to establish the commission of a criminal offence seems to be lacking in the instant case.

Section 79 of the IT Act may also be deployed in Baazee's defence. Section 79 expressly states that a network service (an intermediary) shall not be liable for any offence for any third party information or data made available by it if it proves that the offence was committed without its knowledge or that it had exercised due

diligence to prevent the same. Moreover, the proviso to section 7 of the IRWP Act exempts a company and its principal officer from liability if they are able to establish that they lacked knowledge of the offence and had exercised due diligence to prevent the commission of the offence. While these two points exempt auction sites and their officers from liability if they lack knowledge, they still have the burden of proving such lack of knowledge on the accused, contrary to the principles of criminal laws.

Auction sites are not liable under U.S. law for the auctions of their users due to the immunity granted under two legislations; viz., The Communications Decency Act (CDA) and the Digital Millennium Copyright Act (DMCA). Under the CDA, "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Similarly, the DMCA does not hold a service provider liable for contents on its network if it does not have actual knowledge that the content on the network or system is infringing; in the absence of such actual knowledge, is not aware of facts which makes the infringing activity apparent; or upon obtaining such knowledge acts expeditiously to remove or disable access to the content.

8.7. Conclusion

We may thus, arrive at a conclusion that the cyber laws in India still needs amendment to cover various aspects of cyber crimes. We also have seen that Indian criminal laws do not adhere to *'Actus non facit reum nisi mens sit rea'*. The definition of "due diligence" is yet required to be given in the IT Act. The offences incorporated need to include the definition of the guilty mind within its ambit.

References

1. Kathuria, K.P., *Law of Crimes and Criminology*, Vinod Publication, Delhi, p. 3.
2. AIR, 1970, Punjab, 137.
3. A.G. Vs. Gradlaugh, 1885, 14 RBD 667, CA.
4. 1980, BBCJ 156, (160) Pat),1981, Cr LJ, Civil, 15.
5. AIR, 1982, SC, 709, S-1973, BCJR 51.
6. AIR, 1982, SC, 1181, 1982, SCC (Cri) 459.
7. Indira Dev, S. Shrirama, *Growth of Legal Systems in Indian Society*, ICSSR, New Delhi, 1980, p. 189.

8. Gautam Dharmasutra, XII, 1.
9. Manusmriti, VIII, 279, Yajnavalkyasmriti, II, 215.
10. Manusmriti, VIII, 284, *Ibid.*
11. Chennappa, Subbhappa, 15 Bom LR 393, Saidukhan, AIR 1951, All 21.
12. Emperor Vs Nanak Chand; AIR 1943, Lah. 208 = 52 PLR 331 = 3 DLR, Shimla, 268.
13. Stephen, James Fitzamen, *A History of Criminal Law of England,* Vol. III, 1967.
14. (1889), 22, QBD, 736.
15. (1889), 33, QBD, 68.
16. 1946, IIO JP 317.
17. (1842), 4 M&M 378, (398).
18. Joga Rao, S.V., *Law of Cyber Crimes and Information Technology,* Nagpur, 2004, p. 143.
19. Sonappa Vs. Emperor, AIR, 1940, Bom, 126.
20. Upendra Vs. Emperor, 45, CWN, 633.
21. Panchkori Vs. Emperor, 67 C.L.J., 41.
22. AIR, 1957, All 180; 1957 CNJ L.J., 344; 20 Cri. L.J., 665.
23. Sec. 79, The Indian Information Technology Act, 2000.

9

Investigation in Cyber Crimes: Implications and Challenges

Synopsis

9.1. Introduction

The unique feature of cyber crimes has rendered the traditional procedural laws as archaic and unsuccessful in resulting into conviction. The problems are not associated with procedure of trial only but also extend to investigation and collection of evidences. The traditional rules and procedures of investigation and evidence collection are often of no use in the investigation of cyber crimes. The criminal offence is committed in one country and extend to another country and even to several other countries. The speed and accuracy is also very fast and perfect. The characteristics of cyber crimes have raised several issues and implications in the pre-trial investigation of cyber crimes. The tasks of investigating agency (police) is much challenging which includes prevention of crimes, collection of evidence, production of evidence before courts arrest of accused, security of systems, etc.

9.2. Procedural Aspects

Section 80 (3) of IT Act clearly stipulates that the provision of the Criminal Procedure Code, 1973 shall be applicable, subject to the provisions of this section in the matters of any entry, search or arrest, made under this section. The procedure of trial involves the following aspects :

(i) Pre-trial stage :
  (a) Information about offence;
  (b) Power of Police to arrest;
  (c) Power to conduct search and seizure.

(ii) Charge sheet :
  (a) Production of prosecution evidence.

(iii) Post chargesheet, (v/s, 173 (8) Cr.P.C.).

(iv) Sentencing (v/s, 235 (2) Cr.P.C.).

• ***Information, Investigation and Arrest***

Section 154 Cr.P.C. contains a provision that every information relating to the commission of a cognisable offence, if given orally to an officer incharge of police station, shall be recorded in writing by him or under his direction.[1] Such information shall be entered into a book to be kept by such officer. If such offence is a non-cognisable offence, then no police officer shall make investigation without the order of a magistrate having power to try such case or commit the case for trial.[2]

The earliest information given in the police station regarding an occurrence of crime is known as 'First Information Report (F.I.R.).[3] The following conditions are to be satisfied to constitute an information as 'First Information Report' within the meaning of the section :

(a) It must be an information relating to commission of a cognisable offence.
(b) It must be given to an officer incharge of a police station.
(c) It must be reduced to writing either by the informant (complainant) himself or under his direction.
(d) The information must be read over to the informant if it is written under his directions.
(e) It must be signed by the informant.
(f) The substance of the information should be entered in a book to be kept by an officer incharge of the police station in such a form as the state may prescribe in this behalf, viz., General Diary or Station Diary or Station House Register.

A cyptic message or an anonymous oral message by a telephone which did not in clear terms specify a cognisable offence can not be deemed as F.I.R.[4] Even an entry in general diary on the basis of telephonic message is not F.I.R.[5]

Section 156 Cr.P.C. statutorily empowers the police to investigate into cognisation offence. Such investigation in case of cyber crimes involving contravention of IT Act has to be done by a police officer of not less than the rank of ACP or Dy. S.P. Investigating officers are not under the control of the courts or any judicial authority during the course of investigation. No magistrate, however, has powers either to interfere with or suspend the police investigation into a cognisable offence. Powers of the police are absolute in this respect. The magistrate may, however, intervene if police decides not to investigate the case.

Investigation, which is an extensive process of collection of evidence of a crime, generally begins with the recording of the First Information Report. It has to be done with due care and caution and proceeded with not only methodically but also scientifically in consonance and conformity with forensic sciences. Hence, the police officer should possess thorough knowledge of

not only the science of investigation but about the computer technology to deal successfully with computer related cyber crimes.

The arrest of the accused person is a major step in the investigation and that too as early as possible and interrogate his involvement and commission of offence and record his statement. Section 41 of Criminal Procedure Code deals with the circumstances under which a police officer may arrest without a warrant. The police is within their powers to record confession as given by the accused persons. Although the confession made before a police officer is inadmissible evidence,[6] there is, however, no harm in recording the confession of the accused person by the police in the course of investigation as the same can be made use of as relevant piece of evidence for the recovery of incriminating articles, etc.

All the steps of investigation must be reduced into writing in the case diary then and there without giving any kind of suspicion regarding manipulation or interpolation. It has to be chronologically written because the court has the right to look into it to find the truth or falsity of any claim made by accused with regard to his arrest, recovery of material objects, etc.

Where an accused person surrenders before the magistrate, rather than being arrested by the policy, such surrender also comes within the ambit of "arrest" as envisaged under section 41 to 44 of the code.[7] The power to arrest by police officer under the section, however, cannot be exercised arbitrarily violating accused's fundamental rights and liberty enshrined under Article 21 of Constitution.[8] The victim of an illegal arrest may claim compensation from state.[9] An arrestee has the right to be informed about the grounds of his arrest, to consult his lawyer or near relative or friend and to be produced before nearest Magistrate within 24 hours of his arrest.[10] The use of the word "may" in the section shows that the power of arrest is discretionary and police officers is always bound to arrest an accused for a cognizable offence.[11] The power to arrest under section 41 Cr.P.C. given to the police is not absolute and is not to be exercised in arbitrary manner but in the judicious way.[12]

- *Power of Search and Seizure*

The police officers are empowered under sections 165 and 100, Code of Criminal Procedure to make a search and seize, if

thinks it necessary, any incriminating evidences which relates the crime to the criminal in the course of investigation. The copies of such search and seizure, however, has to be forwarded to the nearest Magistrate. If the thing to be searched for falls within the limits of another police station, the investigating officer can also request the officer incharge of that police station and in such a cases that police officer will conduct the search and forward any seized things to the investigating officer (S. 166). The section 100 Cr.P.C. and 165 Cr.P.C. reads as follows :

Section 100. *Person in charge of closed place to allow search* :

(1) Whenever any place liable to search or inspection under this chapter is closed, any person residing in, or being in charge of, such place, shall, on demand of the officer or other person executing the warrant and production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein.

(2) If ingress in such place cannot be so obtained, the officer or other person executing the warrant may proceed in the manner provided by section(2) of section (47).

(3) When any person in or about such place is reasonably suspected of concealing about his person any article for which search should be made, such person may be searched and if such person is a woman, the search shall be made by another woman with strict regard to decency.

(4) Before making search under this chapter, the officer or other person about to make it shall call upon two or more independent and respectable inhabitants of the locality is which the place to be searched is situated or any of other locality if no such inhabitant of the said locality is available or is willing to be a witness to the search, to attend and witness the search and may issue an order in writing to them or any of them so to do.

(5) The search shall be made in their presence, and a list of all things seized in the course of such search and of the place in which they are respectively found shall be prepared by such officer or other person and signed by such witnesses; but no person witnessing a search under

this section shall be required to attend the court as a witness of search unless specifically summoned by it.

(6) The occupant of the place searched, or some other person in his behalf, shell, in every instance, be permitted to attend during the search, and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person.

(7) When a person is searched under sub-section(3), a list of all things taken possession of, shall be prepared, and a copy thereof shall be delivered to such person.

(8) Any person who, without reasonable cause, refuses or neglects to attend any witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have committed an offences under section 187 of the Indian Penal Code, (45 of 1860).

The search under section: 100(4) Cr.P.C. should be made in the presence of two or more persons of the locality, but one person may be sufficient to prove search and recovery before the court.[1] Recovery opinion shall be doubtful if presence of two witnesses were not ensured at the site of search.[2] A search without arrest is illegal,[3] as search and seizure can be effected only after arrest. Where the prosecution is based on seizure, the provisions of sec. 100 not complied with and even only witness turns hostile, the accused liable to be acquitted.[4]

There are certain subjective and legal formalities thereof which are required to be followed while making a lawful search. Firstly, it provides for the right of free ingress in case of closed premises on demand and on production of the warrant of search by the police officer, and secondly, the search should made fairly and squarely and that there is no "planting" of article by the police. In order to ensure fairness it is required that when making a search, the searching officer should give his personal search to the witnesses before entering the premises to be searched and should similarly

1. Govindram and Govinda-Vs-State = 1984(2) Crimes 937 (Del.);
2. Premchand-V-State of Punjab = 1984 Cri.L.J. 1131;
3. R.K.D. Singh-V-K.K.N.S. Singh =1971 Cri.L.J. 1736;
4. Ram Singh-V-State of Haryana = 1993(1) Crimes 1055;

search witness also in the presence of one another.[13] It is also obligatory that at least two independent and respectable witnesses of the locality should be present. The prosecution case will hardly succeed which is solely based on recovery made as a result of search not witnessed by at least two independent and respectable persons as required by section 100 Cr.P.C. unless it was impractible to procure such witness. It is further required that the occupant of the place searched or his representative should be permitted to attend during the search and to have a copy of the list prepared. When the provisions of section 100 and section 165 of the code are contravened, the search can be resisted by the persons whose premises are being searched.[14]

Where all witnesses belong to the police department and effort was made to associate independent persons of the locality, conviction is unsustainable.[15] It is quite unsafe to rely on the statements of police officials to convict persons wherever independent witness from the locality can be joined before carrying out the search and recovery, but in exceptional cases if the police officer is so trustworthy his evidence can be acted upon.[16]

But non-compliance of the provisions of sub-section (4) of section 100 shall not be fatal to the prosecution in all circumstances. Each case has to be judged on the basis of merits of each case. If seizure witnesses are not respectable persons of the same locality but from another locality, it may amount only an irregularity, not affecting the legality of the proceeding.[17]

The provisions of section 100 is applicable only in case of search of place and hence its compliance is not necessary in case of search of shoes worn by the accused or a motor car or a person.[18] If a search has been in contravention of section 100 and section 165 of Cr.P.C., it would not vitiate seizure of articles, nor the subsequent steps in investigation or proceeding would be vitiated or affected in any manner.[19]

The provision of section 165, Code of Criminal Procedure is mandatory and therefore, recording of reasons of the official act is necessary.[20] For applicability of section 165, Code of Criminal Procedure, four conditions are imposed :

1. The police officer must have reasonable ground of believing that anything necessary for the purpose of an investigation of an offence cannot, in his opinion, be

obtained otherwise than by making a search, without undue delay;

2. He should record in writing the ground of his belief and specify in such writing as far as possible the things for which the search is to be made;
3. He must conduct the search if practicable, in person then, and
4. If it is not practicable to make the search himself, he must record in writing the reasons for not himself making the search and shall authorise a subordinate officer to make the search after specifying in writing the place to be searched, and so far as possible the thing for which search is proposed to be made.

If the search is made in the contravention of provisions contained in the section 100 and section 165, Code of Criminal Procedure, the search will be illegal in the eye of law.[21] If no copy of seizure list, or recovery memo, has been furnished to the accused, this fact shall go against the prosecution.[22] The provisions contained under section 100 (4), Code of Criminal Procedure is mandatory and if no independent witnesses were called before making a search, then veracity of official witness would not be believed. Mere gravity of offence cannot be a decisive factor in violating such mandatory provisions of law.[23]

- ***Issue of Processes for Production of Things or Appearance of Accused***

According to section 91 of Code of Criminal Procedure, when a police officer incharge of a police station considers that production of any document or other thing which is necessary or desirable for the purpose of any investigation, he may issue a written order to the person in requiring him to produce it at the time and place stated in that order. If document or thing in the custody of a postal or telegraph authority, then only a commissioner of police or a District Superintendent of Police can require the postal or telegraph authority to detain such document, etc., pending an order for production from a District Magistrate, a Chief Judicial Magistrate or a court of session or High Court.[24]

Any court may also pass an order or requisition to produce or detain a thing to the person whom such order or requisition has been issued and it is believed that he will not or would not

produce the document or thing, and court may also issue a search warrant directing any officer of police to inspect or make search.[25] A person incharge of a closed place where the proposed search is to be carried out by a police officer has a duty to allow the search.[26]

Succeeding Magistrate had power to issue process in a complaint of which "cognisance had earlier been taken by his predecessor.[27] However, no process under section 204 (2) can be issued by a court unless prosecution files list of witnesses.[28]

• ***Submission of Charge Sheet***

The investigative police officer collects required evidences sustainable by the court of law and submits charge-sheet along with a detailed report as envisaged under section 173 Cr.P.C.

The provisions of sections 173 Cr.P.C. records as follows :

Section 173. Report of police officer on completion of investigation:

(1) Every investigation under this chapter shall be completed without unnecessary delay.

(2) (i) As soon as it is competed, the officer-in-charge of the police station shall forward to a magistrate empowered to take cognizance of the offence on a police report, a report in the form prescribed by the state government, stating-

(a) the names of the parties;

(b) the nature of the information;

(c) the names of the persons who appear to be acquainted with the circumstances of the case;

(d) whether any offence appears to have been committed and, if so, by whom;

(e) whether the accused has been arrested;

(f) whether he has been released on his bond and, if so, whether with or without sureties;

(g) whether he has been forwarded in custody under section 170;

(ii) The officer shall also communicate, in such manner as may be prescribed by the state Government, the action taken by him, to the person, if any, by whom the information relating to the commission of the offence was first given.

(3) When a superior officer of police has been appointed under section 158, the report shall, in any case in which the state Government by general or special order so directs, be submitted, through that officer, and he may, pending the orders of the magistrate, direct the officer in charge of the police station to make further investigation.

(4) Whenever it appears from a report forwarded under this section that the accused has been released on his bond, the magistrate shall make such order for the discharge of such bond or otherwise as he thinks fit.

(5) When such report is in respect of a case to which section 170 applies the police officer shall forward to the magistrate along with the report—

(a) all document or relevant extracts thereof on which the prosecution proposes to rely order than those already sent to the magistrate during investigation;

(b) the statement recorded under section 161 of all the persons whom the prosecution proposes to examine as its witnesses.

(6) If the police officer is of opinion that any part of any such statement is not relevant to the subject-matter of the proceedings or that its disclosure to the accused is not essential in the interest of justices and is inexpedient in the public interest, he shall indicate that part of the statement and append a note requesting the magistrate to excludes that part from the copies to be granted to the accused and sitting his reasons for making such request.

(7) Where the police officer investigating the case finds it convenient so to do, he may furnish to the accused copies of all or any of the documents referred to in sub-section (5).

(8) Nothing in this section shall be deemed to preclude further investigation in respect of an offence after a report under sub-section (2) has been forwarded to the magistrate and, when upon such investigation, the officer in charge of the police station obtains further evidence, oral or documentary, he shall forward to the magistrate a further report or reports regarding such evidences in the form prescribed; and the provisions of sub-section (2) to (6)

shall, as far as may be, apply in relation to such report or reports as they apply in relation to a report forwarded under sub-section (2).

There are three kinds of investigation reports to be submitted by the police officer at different stages of investigation : (i) A preliminary report required to be submitted by police officers or officers incharge to the magistrate under section 157 Cr.P.C.; (ii) section 168 requires a report from a subordinate police officer to the officer incharge of the station, and (iii) a final report under section 173 Cr.P.C. submitted by the police officer as soon as investigation is completed to the magistrate. The delay of seven years was held to be a good ground for setting aside the order of conviction[29] as accused's rights of speedy trial envisaged under Article 21 of Constitution includes investigation also.[30]

Magistrate is not bound to accept the report submitted after the conclusions of the investigation. Even if a police officer submits a charge sheet on investigation directed to be made under section 202 (1), Code of Criminal Procedure, such report will be treated as a report under section 202 (1) and the magistrate would proceed with the case as it is proceeded on complaint.[31] The investigation must be made speedily as delay in investigation assists an accused to square up the investigation.[32]

If a Magistrate is not satisfied by the final report submitted, then it may order for re-investigation as successive investigations are permissible in section 173 (8), Code of Criminal Procedure.[33] Even after the Magistrate has taken cognisance of an offence, if fresh facts come to the light which require further investigation, police can investigate again and file a subsequent charge sheet.[34] But after cognisance of offence was taken by the Magistrate on receipt of police report, the police could not further investigate into offence without permission of the Magistrate.[35] The Magistrate has a power to accept further documents even before the charge is framed provided they are relevant and admissible in evidence.

- ***Production of Additorial Evidence during Trial***

"173 (8). Nothing in this section shall be deemed to preclude further investigation in respect of an offence after a report under sub-section (2) has been forwarded to the Magistrate and whereupon such investigation, the officer incharge of

police station obtains further evidence, oral or documentary, he shall forward to the Magistrate a further report or reports regarding such evidence in the form of prescribed; and the provisions of sub-sections (2) to (6) shall, as far as may be, apply in relation to such report or reports as they apply in relation to a report forwarded under sub-section (2)."

Police may conduct further enquiry even after filing a final report and such power is vested in them under section 173 (8) Cr.P.C. Even after the cognisance has been taken by the court on the basis of report first submitted, police may continue to investigate a case further.[36] It is open to the court to direct further investigation even after cognisance was taken by the court[37] and further no assignment of precise reason is necessary.[38] The court cannot give any direction to the investigating officer restraining him from further investigation if such investigating officer has sufficient and valid grounds to continue investigation.[39]

Sub-section (8) is a new provision which empowers a police office to make further investigation on the basis of new materials,[40] and file supplementary charge-sheet to the court. Such supplementary charge-sheet, however, cannot be submitted, without making further investigation and obtaining further evidences.[41] The court of session has got power to direct further investigation under sec. 173 (8) Cr.P.C. Further, investigation can be conducted by the same agency and not by a different agency.

The Magistrate is not barred to the law from taking cognisances for the reason that he has accepted final report.[42] After taking cognisance of an offence, the Magistrate cannot pass an order for further investigation under section 173 (8) by CBI unless the police submits a formal application seeking further investigation.[43] After cognisance has been taken by the court on the basis of case diary and *prima facie* case, subsequent reopening of investigation without any reasonable basis or material on record is illegal and unsustainable in law.[44] The investigating officer has no unfettered power to re-investigate without sufficient evidence to proceed against.[45] The investigating officer may add more accused when there is adequate material and evidence. But he has to assign reasons by a speaking order.

• *Evidence while Awarding Sentence*

Under section 235 (2) Cr.P.C., the investigating officer may adduce relevant evidence to sustain a particular form of punishment if the court records conviction.

The provisions of section 235 Cr.P.C. reads as follows :

"235 (1) *Judgement of Acquittal or Conviction* : After hearing arguments and points of law, if any, the Judge shall give a judgement in the case. (2) If the accused is convicted, the Judge shall, unless he proceeds in accordance with the provisions of section 360, hear the accused on the question of sentence, and then pass sentence on him according to law."

The provision in clause (2) is new and envisages that after a court holds a person guilty, it must consider the question of sentencing in the light of various factors such as the prior criminal record of the offender, his age, employment, educational background, home life, sobriety and social adjustment, educational and mental condition, and the prospects of his returning to the normal path of conformity with the law. This provision provides an opportunity to the accused and the prosecution to present points of view. On the question of sentence the Court is also bound to give them opportunity of hearing on the point of sentence and this provision is mandatory.[46] Non-compliance of this provision may be a ground for retrial on the question of sentence only. The session court has to hold a *de novo* trial if such a case is remitted back to the court only on question of sentence. But such remand is likely to cause delay, the appellate court may also provide the opportunity of hearing to the accused on the question of sentence to avoid further delay.[47]

The opportunity of hearing is not confined to oral hearing only. Both prosecution and accused are entitled to produce materials to establish their submission.[48] The state being the prosecutor must be called upon to submit before the court as to which sentence would be appropriate in view of facts and circumstances of the case. The accused's hearing on the question of sentence is obligatory.[49] Hearing on the quantum of sentence is necessary in the cases of grave offences.[50] Since hearing of accused convicted in an offence is mandatory, conviction is liable to be quashed if such accused is not heard on the question of sentence[51] and the case may be demanded for hearing. It is not necessary for

the court to adjourn the hearing of the case to some other day for the purpose of hearing the accused on the point of sentences. It is, however, discretion of the court and it may allow adjournment to the prosecution or the accused in cases where death sentence is proposed to be inflicted. The courts are empowered to record conviction and sentence on the same day. Where the compliance of the provision of sec. 235 (2) would cause further delay, the sentence already undergone by the accused convict was held sufficient.[52]

9.3. Issues, Complications and Challenges Concerning Cyber Crimes

Information technology is increasing being used in all sectors of the economy including industry, commerce and service sectors such as Government. With liberalisation and globalisation of the Indian economy, computer-based information system are growing fast. The legal and security implications of this globalisation of information are being examined by the author. A plethora of legislations in India require recasting to accommodate these changes.

Information technology today has evolved from a supporting function to become a part and parcel of the overall management concept. To improve the quality of services and products delivered, human resources in India in all organisations will have to be trained for use of information technology.

Major steps have been taken up by the Government of India in the direction of implementation of information technology in vital sectors of economy, management and development. This throws up various security issues involved in the implementation of the same especially considering the fact that India is a vast country of multi-cultural, multi-racial and multi-lingual citizens with various levels of development and exposure to knowledge.

- ***Need of IT Security in India***

India has achieved tremendous developments in the field of production and use of electronic hardware and improvement in communication. This could happen due to change in government policy during the period 1985 to 1987. The new policies were dedicated for development of various networks like SAILNET, COALNET, DILCOMNET, POWERNET, ERNET, I-NET and

INTERNET and these networks have become operational using various communication media. The economic, financial and social development works initiated by the Government of India opened up many new avenues demanding globalisation of Indian industry. This demand certain legislative measures to be initiated and adopted to safeguard against insecurity and illegal accesses and abuses of computer-based information systems.

The statutory organisation like the Bureau of Indian Standards (BIS) has recognised the developments of electronic and communications technology in the country. Further, in 1988 it recognised the divisional councils to work out guidelines and standards in all areas of information technology. In view of increasing importance of information technology, a separate committee LTD-38 was set up to work out information security guidelines and standards. The Computer Society in India, an organisation of computer professionals, also set up separate sub-groups to workout necessary guidelines and for creating awareness of information security. The International Federation for Information Processing (IFIP) also reorganised their own technical committees and set up a separate committee TC-11 to look into this area.

- ***Sceneraio in Developing Countries and Security Friendly Legislations***

In the developing countries, the impact of technology is being slowly felt and computers are being installed in every office of government and private organisations. With the rapid development in the field of communication facilities, data communication is also growing at a faster pace. Developing countries face the problem of discontinuing the manual processes and depending on computer-based information systems. There is apparent lack of confidence in use of automated systems for decision-making in the industrial, corporate and Government sectors. The dependency of counter based information in the decision-making process is increasing slowly. This needs support for security based legislation. Developing countries on the one hand face the problem of employment generation and on the other hand face the problem of demand of services using new technologies. Without these new technologies, they cannot provide effective and efficient services at a lower cost with reduced level

of human interaction. The large scale involvement of multinational and globalisation of economies necessitate that every country be dependent on other countries for certain products and services.

Three factors are necessary to be considered for developing countries so that they may compete with developed countries :

(a) Production of quality products at the lower costs.

(b) Provision of quality services, efficiently and effectively.

(c) Globalisation of economies and export thrust to improve the balance of trade and balance of position.

The impact of this new technology application necessitates the legislation of new Acts or Amendments to existing Acts. Security based legislation is nowadays an important issue to be discussed among all concerned for reclassification of information to be made available to eligible classes of people and to legally prosecute and punish the others who illegally access and abuse the information for their own benefits.

• *Scenario of India*

In the Indian context, the 'Evidence Act' does not recognise computer produced documents including computer oriented microfilm as an admissible evidence. 'Indian Customs Act' has been amended to accept computer based microfilms of the shipping bills made by the customs authority to be accepted by customs tribunals as an evidence. 'Bankers Books of Evidence' still awaits necessary amendments so that copies produced through computers containing customers accounts may be admissible evidence in the courts of laws. Ever through India has launched national clearing mechanism, the microfilming of cheques and financial bearing instruments passing through the clearing houses is not being practical due to the existing 'Negotiable Instruments Act'. In developed countries, microfilm copies of the front and back sides of the cheques done by the clearing house is a proof of fund transfer between two accounts. In India, some changes in the Negotiable Instruments Act are still required to ensure that funds transfer takes place faster than physical movement of money bearing instruments. At present in India, Banks keep cheques in safe custody as a proof of evidence of transactions for about ten years. But in developed countries, cheques are sent for the respective account holders for necessary action from their side, if

there is any fraud with the cheques. This will also be considered in India provided a copy of the cheques are available in the clearing house or at the bank on a machine readable media, which can be accessed at any point of time, as required. The information stored in any electronic media has got certain storage life and such information can be retrieved at any point of time. Although the statutory period of the retention life of electronic media is quite long, yet it is now necessary for us to amend the 'Archival Act' or introduce a new 'Electronic Archival Act' for storage of information preserved on electronic media. Such arrangement is necessary since all important information pertaining to trade, industry and finance is going to be stored on electronic media using computer technology. There should be standard guidelines for storage and release of such information from the archive media.

The rapid improvement in the field of electronic media has enabled to send electronic mail and integration of voice, image and data through the communication networks quickly from one part of the world to another. This situation has given birth to a new challenge—to identify the accessor and authorising him to access the information stored in multiple locations which are connected through communication channels. The development of digital communication technology and high speed transmission system enable people to preserve information at their respective places and make it available through public communication media transmitting and receiving information including images very fast. The concurrent impact of the technology necessitates the enactment of the 'Illegal Access or Abuse Act' as a strong legislative measure to provide safeguards for unauthorised access and to identify the accessors authorised and unauthorised by means of different technologies and through access control mechanism. Illegal access and abuse are to be made punishable by the law. In developed countries, such crimes are on increase leaps and bounds and situation should alert the developing countries where technologies are slowly making an impact. Appropriate and adequate safeguards for classified information have to be ensured.

Information is now regarded as an important property in the present days of technological situations. It is, therefore, to initiate enactment of an 'Information Protection Act' for safeguarding

stored information and to ensure that information is not abused by authorised persons for the purpose other than for which it was collected. Indian Penal Code also requires necessary amendments to tackle with the illegal use of information technology in industry, commerce and Government as will as private sectors and to deal with hi-tech cyber crimes.

The protection of privacy is another challenge with us. According to various Government regulations and requirements, citizens are required to submit their personal information to various authorities for specific purposes. It is imperative that such information should not be used for purpose other than for which it is submitted. Recently, a Delhi based lawyer filed a petition before the Supreme Court, asking it to ban unsolicited telemarketing calls to consumers as they were an "invasion of privacy and violation of the right to live a peaceful life",[53] when the court issued notices to the government. It is therefore, now imperative to enact, an Anti-piracy and Privacy Protection Act, the save the interests of people and for protection of the privacy of information. Some of the provisions for protection of piracy are already available in 'India Copyright Act', but these provisions are now not adequate enough to deal with the present situation. The rapid development in the field of multimedia and voice and video technologies provides further challenges for legislators.

IT auditors or information system certificate specialists help in quality certification and educate management in information system vulnerabilities and help to provide adequate safeguards in operations and control. Audit of information systems is an important area for maintaining information security. Information technology audit consists not only of financial audit but also systems, technology and operations audit. New standards such as ISO-9000 enable certification of the systems and processes and certify quality. The certification professional update their technologies and tools of certification so that quality is maintained and total quality management becomes a management commitment in every organisation. Information technology industry is posing a new challenge for these quality assessors and auditors as this technology is growing at a fast rate and integrates electronics, entertainment, and business functions and provides a tool for human being to improve their standard of

living by adopting these technologies. Information security administration requires a new class of professionals who will be in a position to advice, and certify that the technologies in use for day-to-day decision-making process are foolproof and that adequate safeguards are introduced for prevention of malpractices and abuse.

The telecommunications infrastructure is the backbone of the present-day technology and opening up of Indian telecom industry is posing a greater challenge in giving legal protection to various players who have entered into joint venture of agreement for providing these services in India. Appropriate amendments in the Indian Telegraphy Act have become essential in view of present services requirements such as value added service, basic telecom services, inter-metro services, intellectual services, mobile communication, communication frauds, etc.

The GATT agreement entered into by India requires changes to Patent and Trade Marks law and 'Copyrights Act' to give proper protection to intellectual property. Computer softwares are also under the purview of intellectual property and, therefore, is covered under the patents and copyrights law. Software theft and software piracy should now be made punishable under the law. National Association of Software and Service Companies (NASSCOM) has taken a lot of initiative in countering software piracy and in training Indian Police in conducting raids to detect software piracy. Software piracy in India is estimated at 95% resulting huge amount of less to exchequer.

More teeth should be given also to the 'The Consumer Protection Act' and 'Unfair Trade Practices Act' in order to support globalisation perspective. There is need of some amendments to the 'Company's Act' to cover the freedom to access company information and also to define boundaries limiting this freedom. Judicial system should also be adequately reformed and judicial officers should be trained to understand the legal implications of high-tech-oriented systems and techniques.

Special care should be taken to solve the legal problem coming to the transborder information flow, which are largely based on the principle of collection limitation, data, quality, purpose specification, use limitation, security safeguard, openness, individual participation and accountability.

9.4. Problems and Precautionary Measures for Investigation

Computer crimes require adequate expertise for investigation by expert investigating officers. So, the collection of evidence and investigation should be made by an investigating team to carry out computer crime investigation with personal skill and expertise.

The investigation must begin with a careful check of all records such as computer system, documentation, system, logs, background and operational information about the organisation and its personnel. If a suspect has been identified, it would be easy to find out the equipment the suspect has used to commit the crime and the depth of his expertise. The records of telephone calls may also be valuable. Investigation should also cover a search for the details of electronic media, equipment and communication used by the organisation. Informants may be able to provide valuable information about the potential suspects and their activities apart from identifying the equipment used to commit the crime and the co-conspirators and other associates. Both physical and electronic surveillance of a suspect may be done to validate information received from the informants. If telephone access codes have been used during the crime, use of pin registers or dialled numbers recorders may help in gathering relevant documentation.

Electronic evidence in any computer-generated data, that is relevant to a case, includes e-mail, text documents, spreadsheets, images, database files, deleted e-mail and files, and backup. The data may be on floppy disk, zip disk, hard drive, tape, CD or DVD. Electronic discovery involves the following steps :

(a) Identification of likely sources.
(b) Collection of electronic evidence avoiding spoliation and maintaining the chain-of-custody.
(c) Making collected data readable and useable.
(d) Filteration of data to achieve a relevant, manageable collection of information.
(e) Making the information available in tiff or PDF format, as part of a database, from a web based repository.

The investigating team should have a special purpose evidence collection kit consisting of diskettes for the storage of files copied from the computers being searched, cassette tapes

drives or hard disks for mass copying or back up of contents of hard disk, a set of utility computer programmes to retrieve and copy data files which can be used to retrieve and copy data files, operating manuals and instructions for various operating systems and programming languages, computer stationery for the printers, sterile operating systems diskettes (which are free from risk of data getting corrupted when crackers programme their diskettes in such way if someone else boots the system all evidence will be destroyed), pen registers that can be used to download codes and members stored in the resident memory of the computer, modem or programmeable telephone, camera equipment to video tape and photograph, the scene, an anti-virus programme to protect the system under investigation from any possible contamination by any other tool used by the investigator and set of adhesive colour lebels, evidence tapes, seals, packing material, marking material, tags, etc.

All the relevant materials should be collected from the place of occurence, including :

(a) All hardware found at the place of occurence.
(b) All software found at the scene of crime.
(c) Computer diskettes, tape and other storage media should be used.
(d) All documentation found at the place of crime.
(e) All periphered equipment including printers, modem, cables, etc., should also be collected.
(f) Any discarded documentation, printouts, printer ribbons and trash collected from waste bins.

The investigating officers, however, should follow certain guidelines[54] while handling the potential evidence. Some do's and don'ts are as follows :

Do not

(a) Disconnect the power before evaluating the overall problem.
(b) Touch the keyboard as far as possible.
(c) Change the computer's current state (do not abandon the programme).
(d) Disconnect the telephone or autodiallers from its source.

Do

(a) Videotape the scene to document the system configuration and the initial condition of the site on your arrival and the condition of the equipment you see.

(b) Photograph the equipment with its serial number, model number and wiring scheme.

(c) Label all evidence so that the cables and other equipment can be reassembled in the same exact configuration.

(d) Write protect at diskettes at the scene and make sure that they are labelled.

(e) In case of a mainframe computer, secure the equipment and determine relevant parts of hardware and software that require close scrutiny and than collect the same. Connect a dialled number recorder to telephone or auto dialler for tracing the intruder. Place an outgoing call recorder through each autodialler or telephone number storage board and obtain a printed record of the stored telephone number or telephone access codes within the resident memory.

The following auditing tools and utilities can be used depending upon the nature of investigation :

(a) Test data method which modifies the processing accuracy of the computer application systems.

(b) Integrated test facility which reviews those functions of auto applications that are internal to the computers.

(c) Similar situation which processes live data files and simulates normal computer application processing.

(d) Snap shot which takes a picture of a computer memory that contains the data elements in a computerised decision making process at the time the decision is made.

(e) Mapping which assesses the extent of computer testing and identifies specific programme logic that has not been tested.

(f) Check sums provide a numerical value to the execution module that can be compared to late suspected modules.

• *FBI Guidelines for Preserving and Submitting Computer Evidence*

The Computer Analysis and Research Team of FBI

Headquarters Lab Washington DC has issued the following guidelines useful for the investigators :

(a) For wrapping the equipment or media, anti-static plastic should be used.

(b) Before wrapping, all the equipment should be disconnected from power and should be brought to room temperature.

(c) Since the physical machine might not actually be a part of the evidence, a copy of the hard disk should be mad first to conduct major part of the investigation.

(d) The Central Processing Unit (CPU) should be thoroughly checked and the hard disk drive read/respite hard should be secured with appropriate software commands. The drive should not be removed from the computer. The monitor and the CPU should be separately wrapped after duly labelling each part including cables and part. The keyboards should be separately packed. Any external or removable hardware, floppy diskette devices should be wrapped separately after proper labelling.

(e) In case of printers and plotters, the dip switch settings should be noted and the ribbon removed carefully as it may provide information on most recent text printed. The modems and other coupling devices should be disconnected from the telephone and label should be placed on both ends of cables describing the connection to PC, printer, modem, etc., and then wrap it as usual.

(f) The magnetic media such as floppy diskettes, hard disks and others should be wrapped in plastic covers because of the risk of static electric discharge. The label indicating "keep away from X-rays and magnetic fields" should be affixed.

(g) All manuals, hardware, notes, loose sheets, pads and other documents should be handled with gloves to preserve the latent finger prints for examinations. Similarly, the print outs, listings should also be carefully handled for latent fingerprint examinations and all these items can be packed in card board boxes.

• *Examination of Computer Evidence*

After following the rules of chain of custody of evidence actual examination can be undertaken in the following steps :

(a) Mark and initial each piece of evidence and segregate them for undertaking different types of studies such as accounting, latent fingerprint examinations, cryptography record verification and other minute analysis.

(b) Instead of using the suspect system disk and the software, the investigator should use his own system disk to examine the computer.

(c) If the system involved in the computer crime is operational, check to determine if the system is fully operational at the time of seizure if not, take logical steps to make the system operational.

(d) Write protect all diskettes, identify the computer to be used for examination, convert the operation system, if necessary, create directory or subdirectory testing and check for hidden or deleted files using custom software and take a print out of all files.

(e) After making a detailed analysis in conjunction with related data obtained from various sources and observations made during analysis, prepare a report documenting the process adopted for analysis in a chronological order.

(f) The report should include the printouts and other observations and conclusions on each of the prints raised in the investigation. Finally, repack all the hardware as packed initially.

Standard tools such as compilers, assemblers, disassembles and debuggers are required for reverse engineering of software that is essential for interpretation of evidence. Digital storage oscilloscope and logical analysers to computer hardware and communication protocols are required for reliable and non-destructive analysis of hardware evidence.

• *International Organisation on Computer Evidence (IOCE)*

The International Organisation on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning

computer crimes investigation and other computer-related forensic issues. Comprised of accredited government agencies involved in computer forensic investigations, IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendations for consideration by its member agencies. In addition to formulating computer evidence standard, IOCE develops communications service between member agencies and holds conferences geared towards the establishment of working relationships.

In response to the G-8 communique and action plans of 1997, IOCE was tasked with the development of international standards for the exchange and recovery of electronic evidence. Working groups in Canada, Europe, the United Kingdom and the United States have been formed to address the standardisation of computer evidence.

During the international Hi-tech Crime and Forensic Conference (HCFC) of October 1999, the IOCE held meetings and a workshop which reviewed the United Kingdom Good Practice Guide and the SWGDE Draft Standards. The working group proposed the following principles, which were voted upon by the IOCE delegates present with unanimous approval. The international principle developed by IOCE for the standardised recovery of computer based evidence is governed by the following attributes :

(a) Consistency with all legal system.
(b) Allowance for the use of a common language.
(c) Durability.
(d) Ability to cross international boundaries.
(e) Ability to instill confidence in integrity of evidence.
(f) Applicability of all forensic evidence.
(g) Applicability at every level, including that of individual, agency and country.

The principles were presented and approved at the International Hi-Tech Crime and Forensic Conference in October, 1999. They are as below :

(a) Upon seizing digital evidence, action taken should not change that evidence.
(b) When it is necessary for a person to access original

digital evidence, that personnel must be forensically competent.

(c) All activity relating to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

(d) All individuals are responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

(e) Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Other items recommended by IOCE further debate and facilitation included :

(a) Forensic competency and the need to generate agreement on international accreditation and the validation of tools, techniques, and training.

(b) Issues relating to practices and procedures for the examination of digital evidence.

(c) The sharing of information relating to hi-tech crime and forensic computing, such as events, tools and techniques.

9.5. Conclusion

The advancement of technology has made radical changes in information gathering, information storage, information processing and information disseminations. Though multi-networks connecting multi-located computers through a variety of communication media, whole world has now become a 'global village'. Policing the internet requires knowledge of technology involved. Now police must be equipped properly to counter the meance of cyber crimes through effective tracing, creation of specialised units, necessary legislation, international cooperation. Creation of regional working groups and international steering committee under the leadership of INTERPOL to counter cyber crimes are steps in right direction and need support from everyone, everywhere who is concerned with the global information society.

References

1. Section, 154, Cr.P.C.
2. Section, 155 (2), Cr.P.C.
3. Soma Bhai Vs. State of Gujarat, AIR, 1975, S.C., 1453.

4. Nemai Adak Vs. State, AIR, 1970, S.C., 1566.
5. Kothucola Vs. State of Assam, 1961, Cr. L.J., 424.
6. Section 25, Indian Evidence Act.
7. V. Vishwanathan Vs. State of Kerala, 1971, M.L.J. (Orl) 13, Niranjan Singh Vs. Prabhakar, AIR, 1980, S.C., 785.
8. Kajal Dey Vs. State of Assam, 1989, Cr. L.J. 1209 (Gau.); Bhim Singh Vs. State of Jammu and Kashmir, 1986, Cr. L.J. 1921-1986, Sec. (Cri.) 47, AIR, 1986, S.C. 494.
9. Inder Singh Vs. State of Punjab, AIR, 1995, S.C., 1948-1995, Cr. L.J. 3235-1995 S.C.C. (Ev.) 586.
10. State of M.P. Vs. Sobha Ram, AIR, 1966, S.C., 1910.
11. Deenam Vs. Jayalalitha, 1989, Mad LW (erl) 395.
12. State of Rajasthan Vs. Bhera, 1979, Cr. L.J. 1237.
13. The State of Bihar Vs. Kapil Deo Singh, AIR, 1969, S.C., 53= 1969, Cr. L.J. 279 = 1969, A 11, L.J. 1; Rabindra Nath Vs. State, 1984, Cr. L.J. 1392.
14. Radhakrishna Vs. State of U.P., AIR, 1963, S.C. 822; Karnail Singh Vs. State of Punjab, 1983, Cr. L.J. 1218.
15. State of H.P. Vs. Sudarshan Kumar (a) Kalia, 1989 (3), Crime 608.
16. Islamuddin Vs. State, 1975, Cr. L.J. 841,(Del.).
17. Durand Didier Vs. Chief Secretary, Union Territory, Goa, AIR, 1989, S.C., 1966, State of Punjab Vs. Wassan Singh, AIR, 1981, S.C., 697; Tej Bahadur Vs. State of U.P., 1970, 3 SCC,779; Sunder Singh Vs. State of U.P., AIR, 1956, S.C. 411; R.K. Gupta Vs. State, 1994 (2), Crime, 668 (Del.).
18. Surinder Singh Vs. State of U.P., AIR, 1956, S.C., 411; B.B. Jadhav Vs. State of Maharastra, 1963, 2, Cr. L.J. 694.
19. B.N. Agrawal Vs. Pharmed Pvt. Ltd., 1984, Cr. L.J. N.O.C., 83, (All).
20. State Vs. Lavkush Kumar, 1985, Cri. R. 486; Sanchaita Investments Vs. State of W.B., 1981, Cri. L.J. N.O.C., 96, AIR,1981, Cal. 157, State of Rajasthan Vs. Rehman, AIR, 1960, S.C. 210, 1960, Cr. L.J. 286.
21. State of Rajasthan Vs. Rahman, AIR, 1960, S.C., 210, 1960, Cri. L.J. 28.
22. Chandra Bhal Vs. State, 1984, All. Dand Nirnaya 42.
23. Atma Singh Vs. State of Punjab, 1984 (2) Crimes 164, 1981 All. L.J. 1203, 1984, All Cri. L.R. 147.
24. Section 92, Code of Criminal Procedure, 1973.

25. Section 93 to 100, Code of Criminal Procedure, 1973.
26. Section 100, *Ibid.*
27. M.L. Gulati Vs Birmani, 1986, Cr. L.J. 770.
28. Subal Manda Vs. State, 1974, Cr. L.J. 176.
29. Mihir Kumar Vs. State of W.B., 1990, Cr U 26 (Cal), G.K. Khandelwal Vs. Dy. Chief Controller, 1989 (1) Crimes, 27.
30. Madheshwari Singh Vs. The State of Bihar, 1986 Cr. L.J. 1771, AIR 1986, Patna, 324.
31. Jamuna Singh Vs. Bahadur Sah, 1964 (2) Cr. L.J. 468, AIR, 1964, S.C. 1541.
32. Hazara Singh Vs. State of U.P., 1969, Cr. L.J. 1928, AIR, 1969 S.C. 951.
33. Abhinandan Jha Vs. Dinesh Mishra, AIR, 1968, S.C. 117, 1968, Cr. L.J. 97. Jhauri Mal Vs. State, 1969, Cr. L.J. 5500, R.N. Chatterjee Vs. Havildar Kuer, 1970, S.C. (Ch) 218.
34. State of Bihar Vs. J.A.C. Sadana, 1980, Cr. L.J. 598, AIR, 1980, S.C. 326.
35. State Vs. Mehar Singh, 1974, Cr. L.J. 970, (F.B.) Punjab.
36. Sri Bhagwan Samradha Sreepada Vallabha Venkata Maharaj Vs. State of A.P. AIR 1999 S.C. 2267, 1999 Cr. L.J. 3661, 1999, AIR SCW, 2318, 1999 (5), SCC 246, Jai Ram Vs State of Rajasthan, 2001, Cr. L.J. 3915 (Raj.).
37. S.B. Patel Vs. State of Rajasthan, 2001, Cr. L.J. 3915 (Raj).
38. Leela Das Vs. State, CBI, 2001, Cr. L.J. 3915, (Raj.).
39. Hasan Khan Vs. State of Rajasthan, 1996, Cr. L.J. 4303, (Raj.).
40. D.D. Patel Vs. State of Gujrat, 1980, Cr. L.J. 29, (Guj.).
41. Antony Scoria Vs. State of Kerala,1980, Cr. L.J. 1211.
42. State of Rajasthan Vs. Aruna Devi, 1995, SCC (Cri) 1, (1995), 1 SCC 1.
43. Prithivis Kumar Nag Vs. State of W.B., 1998, Cr. L.J. 3502 (Cal.).
44. Pusparani Sanial Vs. S.K. Biswal, 1998, Cr. L.J. 3764, (Ori.).
45. Kennady Vs. State, 1997, Cr. L.J. 1465 (Mad.).
46. Santa Singh Vs. State of Punjab, AIR, 1976, SC 2386, Dagdu Vs. Maharashtra, AIR 1977, SC 1579, 1977 Cr. L.J. 1206 (SC), M.A. Waheed Vs. State, 1996 Cr. L.J. 1059 (A.P.).
47. Narpal Singh Vs. State of Haryana, AIR, 1977, SC, 1066.
48. Santa Singh Vs. State of Punjab, AIR, 1976, SC, 2386, 1976, Cr. L.J. 1875, Shankar Vs. State of T.N., 1994, Cr. L.J. 3071 (S.C.).

49. Shiv Mohan Singh Vs. State (Delhi Admn.), AIR, 1977, S.C., 1977, Cr. L.J. 767.
50. Narkey Vs. State, 1969, Cr. L.J. 2357, (Ker.).
51. Md. Shafi Bhat Vs. State of J.K., 1996 Cr. L.J. 2046 (J.K.).
52. State Vs. Musa, 1991, Cr. L.J. 2168 (Ori).
53. Outlook, 21 Feburary, 2005.
54. Gandhi, K.P.C., I.G. (Police) and Director, State Forensic Science Lab, Hyderabad.

10

Cyber Crimes : Discovery and Appreciation of Evidences

Synopsis

- *Understanding of Cyber Evidence*
- *Discovery of Cyber Evidence*
- *Search, Seizure and Collection of Evidence*
- *Seizure and Protection of Evidence*
- *Electronic Surveillance*
- *Forensic Examination of Evidence*

10.4. Computer Generated Evidence and their Admissibility

10.5. Judicial Interpretation of Computer related Evidence

10.1. Introduction

The task of collection of evidence and its presentation before court of law is a very important aspect of criminal trial. The prompt discovery, safe custody and presentation of evidence in appropriate and acceptable form is challenge in the matters of cyber crimes. The device used by cyber criminals are more sophisticated than the traditional criminals. The cyber criminal are far more technologically equipped to operate into the devices of computer and related storage and communication equipments. The number of crimes and criminals is increasing leaps and bounds who use computers, laptops, network servers and even cellular or mobile phones in commission of crimes.

The computers are used both as tools as well as the target of cyber crimes. Computers may provide the means for committing crime against a material stored in another computer. For instance, the cyber criminal may use internet to send an illegal e-mail or to conduct a hacking against another computer, or to disseminate computer virus, etc. Computers may also be used as a storage device for evidence of crime. For example, police may coincidently seize a computer containing details of a money launders or drug smugglers. It is therefore obvious that computer besides being a victim as well as weapon of cyber crimes, may be an important piece of evidence in the wake of investigation of a cyber crime and appreciation of evidence during trial.

10.2 Law of Evidence : An Introduction

- ***Evidence : Definition***

Evidence in simple words may be defined as an act or material or anything which is necessary to prove a particular fact. In a suit or proceeding (both civil and criminal) before a court of

law, the judge considers and weighs up the evidences arrive at a conclusion. Evidence placed before courts are of various types, viz., oral testimony, document, instruments or weapons used for commiting a crime or those which are of appreciation of evidences which are peculiar only to the scrutiny of evidence in civil proceedings. In a civil case, the fact may be proved by a mere preponderance of evidence,[1] while in a criminal case the prosecution must prove the charge beyond reasonable doubt.[2]

The term "preponderance of evidence", as defined in *American jurisprudence,* 2nd Edition, Vol. 30, in Article 1164, means "the weight, credit and value of the aggregate evidence on either side and is usually considered to be synonymous with the term greater might of the credible evidence."[3] In simple words, we may say that it means probability of truth.

The term "proved" has been defined under section 3 of the Evidence Act as follows :

> "A fact is said to be proved when after considering the matter before it, the court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists."

The principles of the laws of evidence by and large are the same both for civil and criminal trials, but the way of application is different. The principles are realed directly or indirectly to the offence.

There are certain established principles for production of evidence before courts of law. These principles are popularly known as the law of evidence. The evidences reduced before a judge or a court of law helps them in arriving at a conclusion. The law of evidence is applied where there is a claim and counter-claim about existence of a fact.

- ***Principles of Evidence***

In a civil or criminal trial, a situation arises between the parties when they raise claim and counter-claim about the existence of a fact or facts. In such situation, the rules of evidence comes into play which governs as to in what manner the evidences are to be adduced before the judge concerned in arriving at a rational conclusion about existence or non-existence of a disputed

fact. In India, the law of evidence is mainly contained in the Indian Evidence Act, 1872. The basic rules of evidence for civil and criminal matters are the same.[4] It is therefore, settled in law that the general standard proof required in criminals cases is not different from the standard of proof in civil matters.[5]

Although the definition of the term "proof" does not make any distinction between civil and criminal cases, yet there is difference in view of its impact. There are certain rules regarding effect of evidence in civil and criminal proceedings.[6]

The Hon'ble Allahabad High Court in *Emperor Vs. Janki* case has explained the distinction between the basic rules as to the appreciation of evidence in a civil and a criminal proceeding in a very lucid manner. In civil cases, there are two parties, plaintiff and defendant, who put forward their cases and try to prove them by adducing evidences. The court is bound by the law to decide the case one way or the other. It gives findings in favour of the party whose evidence is more probable. But this does not happen in a criminal trial. In a criminal trial there is no question of two parties proving their cases. In a criminal trial, the prosecution is one and the only party and it has to prove its case and that too beyond a reasonable doubt. In criminal cases no weight of preponderance of evidence is sufficient. In civil cases, both has to prove their cases by placing their evidence before the court and try to prove their cases. If a party fails to prove his case, he would lose. In criminal trial it is the duty of the prosecution to bring all the evidence before the court to prove the charge and the opposite party, as a measure of defence, has to create just doubt in the prosecution evidences.

(a) Best Evidence Rule : The law of evidence is "Best Evidence Rule". The term "best" is used to indicate a relatively preferred evidence in terms of reliability. There is fundamental difference between "Best Evidence Rule" and best rule of evidence. Best rule of evidence is concerned with the nature or character of particular evidence considered for the purpose of arriving at a rational conclusion. But the best rule of evidence deals with rules which regulate the process of presenting evidence in a court not enforced with the same rigidity against a person accused of a criminal offence as against another party of a civil litigation. There are certain exceptions to the law governing the admissibility of evidence

which apply only to criminal trials, and which have attained their form by way of constant and invariable practice of judging when presiding at criminal trials. These rules of providence and discretion have become an integral part of the administration of criminal law and now have acquired status of the full force of law. As a matter of instance, such practice is to be found in the discretion of judges to injuries strongly warning them not to act upon the evidence of an accomplice unless it is corroborated.[7]

Unlike criminal cases, it cannot be said that even in civil cases the benefit of every reasonable doubt must necessarily go to the defendant. The fact that the defendant has failed to prove a positive case which is intended to rebut the plaintiffs case must be given due weight and court cannot require any party to give a conclusive proof of any fact. The standard of proof is that which is given in the Evidence Act.[8]

In a criminal case the court has to rule out the possibility of innocence of the accused when the court is called upon to convict a person having committed any offence. On the contrary, in civil case all that is necessary to insist upon is that the proof adduced in support of a fact is such that it should make a prudent man to act proceeding in common law context. Some of jurists are of opinion that there should be no rules of evidence at because such rule, which regulates the process of adducing evidence in a court of law is in fact a constraint on the judge as it up to a great extent erodes the autonomy enjoyed by the common law judges. But this viewpoint does not enjoy support in India. Indian Evidence Act contains explicit legal rules providing significant guidance to the judges for deciding the relevancy and admissibility of evidence produced before them during a civil or criminal trial and rule out any kind of unpredictability associated with subjective assessments.

(b) Principle of Relevance : The principle if "Relevance" provides guidance to the judges for considering only relevant evidence while deciding a contested fact. Section 5 of the Indian Evidence Act provides that the parties concerned may adduce evidence in a suit or proceeding of the existence or non-existence of every fact in issue. In absence of a statutory provision expressly indicating as such, an irrelevant fact is always inadmissible.

(c) Admissibility : A judge is empowered under section 136 of the Indian Evidence Act to take decision regarding admissibility

of evidence produced before him. The judges may guide a party as to in what manner the alleged fact, if proved, would be relevant and the judge can admit evidence what he thinks to be expedient in the interest of justice. If the relevancy of a particular fact depends upon another fact which is required to be proved first, the judge has got discretion to either allow the evidence of the first fact to be adduced first before the second fact is produced before him or may also require that evidence be given of the second fact before evidence is produced of the first fact.

(d) Appreciation : Every fact, being relevant and admissible, cannot always be construed as proved fact. There may, however, be some exceptional circumstances when a certain fact may be construed as a proved fact, but this may not happen in all circumstances. The appreciation of evidence is a process which facilitates a judge to arrive at a National conclusion. Although the act of arriving at a National conclusion is left at the wisdom, experience and acumen of judges, yet the Evidence Act provides adequate guidance for appreciation of evidences. The process of appreciation of evidence, *inter alia,* includes the examination of witness, impeachment of witness, creditworthiness of witness and corroboration of evidence, etc.

- ***Types of Evidence***

Evidence in their respective circumstances are classified into various types, i.e., oral, direct, documentary, circumstantial, primary, secondary, hearsay, real, scientific and digital. These different types of evidences have their distinctive features and can be produced before a court of law to prove a fact. It is not necessary at all to produce all types of evidences to prove a fact. Even one evidence sometimes may be sufficient to prove a fact. The presentation of such evidences depends upon the circumstances of each case.

(a) Direct Evidence :The statement made before the court by witness, in relation to matters of fact under inquiry and all documents produced for the inspection of the court. Statements of witnesses before court or document would fall under the meaning and the ambit of the term evidence though they do not fall technically within the purview of the word evidence as defined in the Evidence Act.

If the evidence is led about the fact which has been heard or seen, the witness produced before the court must say that he himself heard or seen, as the situation may be, the fact and only evidence shall be deemed "direct evidence". If the evidence produced is about a fact which can be perceived by any other sense or in any other manner, the witness produced must say that he holds that opinion and the grounds on which he holds such opinion. Documents which are produced by the witness in the court are regarded are direct evidence.[9]

(b) Circumstantial Evidence : Circumstantial type of evidence is an indirect type of evidence which accrues out of a peculiar fact or circumstance or situation of case and that is relevant to prove a fact. For example, if a witness says that he has seen the accused killing a person with a knife then it is a direct evidence and if the witness says that he has seen the accused coming out of the room where a person was found dead, then it is a circumstantial evidence. A statement made by a witness before a court must be given an opportunity to the other side to cross-examine to test its correctness otherwise it will not be considered as evidence.[10]

(c) Hearsay Evidence : The "hearsay evidence" is an evidence which is given by a person who has himself not seen the incident but has heard or gained the information from some other source. A news item published in a newspaper is a "hearsay evidence".

(d) Oral Evidence : Oral evidence is the evidence which is given by the words of mouth or gesture and is worthy of credence, with or without any other corroborating proofs, to prove a fact. Oral evidence includes other forms of communication also, for example, statement made by a witness from a foreign country or such distant place through videoconferencing is also evidence. Likewise, a deaf person may give his statements by signs or by writing.

(e) Documentary Evidence : "Documentary evidence" is evidence produced in the form of documents. Document means any thing in written or expressed or described form such as letters, figures or marks, any report or more than one of those means intended to be used for proving a fact.

(f) Scientific or Expert Evidence : Scientific or Expert evidence is a report or opinion of an expert or experts on certain complex issues and facts concerning any scientific issue concerning a fact

and its application to prove a fact. The experts such as medical expert, Ballistis expert, forensic experts, etc., give their opinion in the field of their knowledge and deposes their understanding about an issue or fact of the matter in question.

(g) Real and Digital Evidence : Real evidence is a objectively or externally demonstrable material evidence which is perceivable in nature. The use and importance of digital evidence in judicial proceeding have been increased tremendously due to rapid growth in the field of computer and internet and their impact on human lives. Large scale activities are going on in cyber space and the real evidence are not available and, therefore, the only alternative left is the admissibility of digital evidence.

(h) DNA Technology and Finger Printing : The DNA technology is one of the most recent as well as most reliable techniques being put to use as far as crime's detection is concerned.[11] Deoxy Ribonuclic Acid (DNA) is found in the cells of all living beings including the human body. DNA finger printing profile is unique to individual and its structure varies from individual to individual. The application of DNA has, *inter alia,* the following advantages:

(i) It can be applied to establish the paternity and maternity of the child.

(ii) DNA can be used in identification of sex of human remains.

(iii) It can be used to match organ doners and recipients in case of transplants.

(iv) It can be applied to identify children in swapping cases occuring in hospitals.

(v) It can be used to identify bodies in mass disasters and bodies in multilated conditions.

(vi) It can be used to confirm the identity of a person.

The technique of DNA finger printings, first developed by Sir Alec Jeffery in 1985, may identify a person by the help of bloodstain, semen stains, hair loss with all possible certainty. It is a well known method to identify criminals by means of digital or palmar prints (of finger prints, Gallon systems). Forensic biology, the testing of biological evidence material, has also advanced dramatically within few years.

DNA finger printing is useful in the cases of exchanges of

babies, rapes, murders, assassinations, paternity related disputes, inheritance, etc. Identity of a criminal is determined by comparing the accused person's DNA fingerprint with that of the blood or semain stain found at the scene of crime. If the DNA finger prints are identical, there is an absolute identification. Using this technique, the Federal Bureau of Investigation (FBI) has successfully concluded on 17th August 1998, the day of Mr. Clinton's testimony before the grand jury, that the stain on the dress of Monica contained Mr. Clinton's DNA, say that there was only on in 7.87 trillion chance that it was not.[12]

Since DNA profiling is the most reliable scientific technique and it can revolutionise the criminal justice procedure, it is, therefore, now necessary that a uniform DNA legislation in this connection should be adopted in India. It requires appropriate amendments and insertion of new sections in Indian Evidence Act, Code of Criminal Procedure and Indian Penal Code.

10.3. Evidence in Cyber Crimes : Challenges and Implications

It is difficult for the police officer investigating a cyber crime to discover and collect evidences of crimes committed against, or by means of them. It is just because the culprit can easily delete a file in a computer and thereby make the data not available to any investigator for evidence. Unlike other crimes of real world, there may not be any tangible evidence available such as weapon, paper, records, etc. The science of computer forensic, however, is developing fast to tackle with the situation, the challenges and implications involved in the collection and presentation of evidences.

- ***Peculiarity of Cyber Evidence***

Usually the culprits delete the materials used in a cyber crimes soon after committing the offence. But technically it is very difficult to remove the materials completely from the computer. The modern computer forensic scientists are now capable to restore the evidences even after it was intentionally deleted. Computer forensics is the science and technology of finding evidences from computer systems and it involves the process of methodically examining computer system for evidence. It is technically a process for recognition, collection, preservation, analysis and presentation of cyber evidence.

Unlike the evidences of real world, the first step involved in the cyber evidence is the discovery followed by collection of evidences. The people at large are still reluctant to report about the occurrence of cyber crimes. Due to their such reluctance, the reporting of cyber crimes, despite being rare, are usually much delayed which causes problems with the investigator.

- ***Preservation of Cyber Crime Evidence***

The process of evidence of cyber crimes is a delicate and precise process. Even minor carelessness may result into destruction of valuable evidence, like collection of finger prints in case of robbery or murder. Only properly skilled and trained person should attempt to collect and preserve evidences. In the matter of a cyber crime, the computer forensic experts and criminal investigators conduct the recovery process by gathering of evidences and restore normal operation by a relatively a smooth exercise. If computer forensic or trained investigator is called promptly he can collect the complete image of the compromised system without delay or loss of valuable time. Till recently, in the wake of preserving cyber crime evidence in the victim's system of hardware were used to be removed and examined. But now computer investigators simply copy the evidence they need without disruption of person's or organisation's system.

- ***Understanding of Cyber Evidence***

Understanding the evidences involved in cyber crimes is a matter of experience and expertise. The evidence concerning cyber crimes may be physical or logical. The media and the hardware components which contain the data are in the category of physical evidence. This physical side of computer forensic involves the process of search and seizure of computer evidences. In the process of search and seizure, an investigator, soon after getting information, rushes to the spot and searches the evidence, takes into custody the computer hardware and media that are involved in a crime. On the contrary, the logical side of computer forensic deals with the extraction of raw data from the relevant source of information. The search operation is done by investigator through log files, searching the internet retrieving data from a database, etc.

- ***Discovery of Cyber Evidence***

The attention of law enforcing agency is focused on the materials of evidences as soon as an occurrence is reported to

them. The computer forensic has an important role to play in the affair of discovery of evidences. It is, however, important to know that computer forensic is not limited to cyber crimes only. Electronic evidences are the important part of evidences in the cyber crimes. The computer may be victim as well as a tool of offence committed. It may also be storage or container of evidences of a cyber crime. The evidence concerning computers vary from the mainframe computer to the pocket size personal data assistant to the floppy diskette, CD or the smaller electronic chip device. It is imperative on the law enforcing agencies to act promptly to seize the evidences as the images, audio, text and other data on these media are easily destroyable or alterable.

- ***Search, Seizure and Collection of Evidence***

The investigator must ensure that the evidences are collected through search and seizure of hardware or through information discovery of logical evidence in a lawful manner. It is important to know that the validity of any evidence in the court of law depends on the legality of the method through which it is collected. A criminal based on illegal search and seizure may be declared illegal in the eye of law.[13] It is, therefore, necessary for the investigator that necessary procedures are followed before proceeding to actual collection. For example, the related provisions of India Evidence Act and Criminal Procedure Code should be followed while making search, seizure and collection of evidences in India.

It is also important to note that according to section 293 of Criminal Procedure Code, reports of certain government service experts can be seed in evidence without formal proof in any inquiry, trial or other proceeding under the code. But if such report has been signed by an officer not within the ambit and scope of section 239 Cr.P.C. then the report could not be read in evidence unless signatory of the report was examined to prove it.[14] Furthermore, one of the formalities required to be observed when making a search is that the searching officer should give his personal search to the witness before entering the premises to be searched and should similarly search witnesses also in the presence of one another.[15]

Section 80 of Indian Information Technology Act, 2000 contains provisions concerning power of police officer and other officers to enter, search, etc., which reads as follows :

Section 80. *Power of Police Officer and other Officer to enter, search, etc.* :

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, 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 authorised 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 the Act.

   Explanation : For the purpose 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 sub-section (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 police station.
3. The provisions of the Code of Criminal Procedure, 1973 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.

Thus, it is clear in the context of Indian laws, that any search or seizure of cyber evidence must be carried out in accordance with the procedure and provisions of Criminal Procedure Code. Only exception has been provided in the Act that the search or seizure has to be made by a police officer not below the rank of Deputy Superintendent of Police or any other officer specially authorised by the Central Government in this behalf. The provisions of search and seizure contained in section 100 of Criminal Procedure Code shall be deemed to be amended to that extent.

- *Seizure and Protection of Evidence*

There are certain precautions which must be taken into consideration by the investigation while making search and

seizure involving the recovering and processing of physical computer evidence from a computer crime place of occurrence. Such precautions are :

(a) Original Evidence should not be Altered : The investigator must take great care and caution to minimise interaction so that no body may alter the original evidence available in the victim or offending computer. It is very difficult to charge the physical and logical state of a computer during interaction. The investigator should avoid to execute programme on a crime scene.

(b) A Suspect should be Kept at Bay from Computer Scene: It is not proper to execute any programme directly such a computer because it may cause damage to the valuable electronic evidences nor should charge the various computer resources, i.e., memory, swap files, the file system, etc. The computer's operating system much potentiality of causing damages of valuable data due to its housekeeping abilities. A suspect must be kept away from computer because he may cause to disappear electronic evidence quickly. The suspect therefore should not be allowed in any circumstances to interact with the crime scene computer or computer components.

(c) Proper Storage of Computer Evidence : The proper storage of computer evidences concerning a computer crime is essential. There are many devices which may help in storage of computer evidences. Some of such devices are wireless telephones, electronic Paging devices, fax machines, caller ID devices, smart cards, etc. Adequate precautions are necessary while accessing to the relevant informations contained in these devices as evidences are also similar to those of computers.

- ***Electronic Surveillance***

The electronic surveillance are also necessary in cyber crimes' investigations. Sometimes the investigator may feel a necessity to keep a watch on the suspected hacker to arrest him red hand or he may set up a cloned e-mail box to keep a surveillance on a suspect sending a hoax e-mail or child pornography, etc. In America, there are specific enactments enabling investigators to keep surveillance. But in India, there is no specific enactment so far dealing with this aspect. There are general provisions in Indian Telegraph Act for surveillance in the telecommunication networks but procedures are complicated one.

• *Forensic Examination of Evidence*

For any computer data to be accepted as an admissible evidence, there may be forensic examination of such data. All the forensic examinations of discovered files must be carried out or backed up copies. These backups should be implemented in a raw, uncompressed format, creating duplicates which should a copy like their originals. The lab evidence which contains details of discovered relevant information such as name of investigator, current date and time, description of each information must be mentioned on the log. Sometimes authentication by investigator is also necessary to confirm that no alteration of electronic data has been made by anyone. There are certain tools which are needed for computer application. These tools are network sniffer (hardware), portable disk duplicator or duplication software, chain-of-custody documentation hardware, cash management software, etc. Forensic examination of electronic evidence has a very important role to play in the field of cyber crimes investigation.

10.4. Computer Generated Evidence and their Admissibility

The second and third schedules to the Indian Evidence Act, 1872 and the Banker's Book Evidence Act, 1891, respectively have been amended to make computer generated evidences admissible in a court of law. The insertion of section 65 A and 65 B in the second schedule are the most important among the amendments which contain special provisions as to evidence relating to electronic records. These sections are as follows :

Section 65-A. Special Provisions as to Evidence Relating to Electronic Record : The contents of electronics record may be proved in accordance with the provisions of section 65 B.

Section 65-B. Admissibility of Electronic Records :

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded on copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question shall be admissible in any

proceeding, without further proof or production of the original, as evidences of any contents of the original or of any fact stated therein or which direct evidences would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:-

(a) The computer output containing the information was produced by the computer during the period over which the computer was need regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly feed into the computer in the ordinary course of the said activities;

(c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information feed into the computer in the ordinary course of the said activities.

(3) Where over any period, the functions of storing or processing information for the purpose of any activities of any regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period, or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

All the computers used for that purpose during that period shall be treated for the purpose of this section as constituting a single computer, and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

(a) identifying the electronic record containing the statement and describing the manner in which it is produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate;

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purpose of this section :

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of these activities, that information, if duly supplied

to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation : For the purpose of this section, any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process;

The case laws are yet to develop in the field of Information Technology Act in India. The interpretation of various provisions of the IT Act, therefore, has to be made according to the natural meaning flowing from it. The recent pronouncement of Supreme Court stating that the recording of evidence through video conferencing is valid in law and under section 273 of Criminal Procedure Code[16], has an appreciable development in the field of appreciation of evidences.

10.5. Judicial interpretation of Computer related Evidence

The proper and appropriate gathering of evidence through investigation is, of course, necessary for success of a criminal prosecution. However, the success of prosecution largely depends upon the appreciation of computer generated evidence by the judiciary. There is need to make judiciary capable of appreciating the tangible evidences as and when they are produced in the court. It is nowadays important that the judicial officer should have a maximum level of knowledge in the computer and network technology in the present days of fast developing cyber age.

Section 46 and section 48 of the Information Technology Act, 2000 provide provision according to which the Central Government is empowered to appoint adjudicating officers who must have the experience in both information technology and legal fields for proper adjudication of any contravention of various provisions of the Act. There is also the provisions for the constitution of a Cyber Regulation Appellate Tribunal for hearing the appeals against the orders of adjudicating officers. But these provisions make it clear that the adjudications of contraventions of cyber regulations should be made by the people of specialised

knowledge. The judge before whom the prosecutions and the defence lawyers are presenting and evaluating the evidences, must be technically competent to evaluate the merits of the evidences as well as the evidentiary value of the document of data produced.

References

1. Cooper Vs. Slade, 1858, 10 E.R. 1488; Manu Pujari Vs. State of Orissa, AIR, 1965, Orissa, 49.
2. Jamal Ahmed Vs. State of U.P., 1979, Cr. L.J. N.O.C., 89, (All), 1979, All Cri. R. 185.
3. Tyagi, S.P., *Law of Evidence,* p. 100.
4. Meena Vs. Lachman, AIR, 1960, Bom. 418, (D.B.).
5. Tyagi, S.P., *Law of Evidence,* Vinod Publication Delhi, p. 100.
6. AIR, 1954, Pepsu 14, I.L.R., 1953, Patiala, 187.
7. King Vs. Chirstie, 1914, Appeal Case, 545.
8. E.V. Rao Vs. Edaora Venkayya, A.I.R., 1943, Mad 38 (2), 207, I.C., 163.
9. Anupam Chakravarty Vs. State of Assam, 1984, Cr. L.J., 733.
10. (1894), I.L.R. Bom, 299.
11. Chugh, Pooja, DNA Technology and its Significance in the Detection of Crime in Modern Society, 2005, *Crimes,* p. 538.
12. *The Times of India,* 24 September, 1998, p. 12.
13. Prem Lal Vs. State of H.P., 1987 (1), Crimes, 323.
14. State of H.P. Vs. E.S. Chareton, 2001 (1) Crimes, 50.
15. The State of Bihar Vs. Kapil Deo Singh, AIR, 196, S.C., 53; 1869, Cr. L.J. 279; Rabindra Nath Vs. State, 1984, Cr. L.J., 1392.
16. State of Maharashtra Vs. Praful B. Desai, 2003 (2), Crimes JT 2003 (3) S.C., 382, 2003 (3), Supreme, 193.

11

Prevention of Cyber Crimes : National and International Endeavours

Synopsis

11.1. Introduction

Cyber crime is not a national problem but it is a problem found all over the world. The international access to information and mobility of data is one of the most important functions of world's economic system. The large scale transaction through computer networks, the ability to access these systems quickly and the opportunity for their abuse through criminal activities have made the computer network systems vulnerable to the criminals. The cyber based commercial transactions world wide is under threat of cyber criminals. The people's privacy and security is also under threat of the cyber criminals.

The world wide occurrences of cyber crimes have created new problems and challenges for the law. Cyber space is fascinating people all over the world. The power is virtually on finger tip and one can easily roam whole world without loss of time. There are no boundaries and restrictions. For youngsters if it is a dreal world then for businessmen it is the fastest medium to deal their contract, on the same pedestals now this space is becoming safest place for criminals due to less accountability.[1] The various cyber crimes such as hacking, cracking, sending obscene mails, tampering of source codes, e-mail abuse, e-mail spoofing, e-mail threat, sending obsence messages over SMS, post defamatory profile on net, mishandling copyright acts, cyber stalking, identity thefts, etc., are increasing leaps and bounds, all around the world.

The United Nations (UNO) has sought for international co-operations to fight against cyber crimes and for finding solutions to the problems of reporting, investigation, discovery and recovery of internet based evidences. The basic objective of increasing the international cooperation is, *inter alia,* to check to potential threat of economic losses and general threat to privacy and other fundamental values created by near-instantaneous cross-border electronic transactions. Various international organisations have initiated to make international efforts to combat cyber crimes.

11.2. International Services on Discovery and Recovery of Electronic and Internet Evidences

Now there are several organisations who are serving the legal field with pride and integrity the high technology of recovery and demonstrating excellence in the field of digital evidence

processing and analysis as well. They are consistently exceeding the customer's expectations and demonstrating the highest character in the examination of information. Their main goal is to provide all individuals, regardless of background, the right of a fair trial. The services of expert consultants are available for both the prosecution and defence.

Electronic evidence is any computer generated data that is relevant to a case. The electronic evidences includes e-mail, text documents, spreadsheets, images, database files, deleted e-mails and files, and backups. The data may be on floppy disc, zip disk, hard drive, tape, CD or DVD.

The discovery of electronic evidences involves the following steps :

(a) Identification of likely sources.
(b) Collection of electronic evidence avoiding spoliation and maintaining the chain-of-custody.
(c) Making the collected data readable and useable.
(d) Filteration of data to achieve a relevant, manageable collection of information.
(e) Making the information available in tiff or PDF format, as a part of database, from a web based respository.

The experts analyse the digital evidence in their own high-tech laboratory, using special software techniques and procedures. Police or investigating officers may send them seized evidence for examination.

The experts conduct a thorough analysis and provide a detailed report outlining the process that was followed and evidence found. Such type of analysis often support investigation in which websites have been visited, which files have been downloaded, when files were last accessed, if attempts have been made to conceal or destroy evidence, and if attempts have been made to fabricate evidence.

Consultant services usually provide the following services regarding cyber crimes :

(a) Computer evidence can be used in any type of criminal prosecution.
(b) Phrasing legally sound language in the affidavit and search warrant.

(c) Seizing the computers properly.
(d) Digital evidence recovery.
(e) Provide quick and thorough examination of victim's computer system.
(f) Inspect computer to see if it is fitted with bombs, booby traps, or hot keys.
(g) Internet pornography evidence.
(h) Complete forensic examination of seized computer hardware and software.
(i) Presentation of the evidence in a format or manner that will be understandable and useable in courts.
(j) Reports that will explain the technical issues or opinion in a manner that can be understood.
(k) Documentation dealing, who, what, why and how information was safely located and recovered.
(l) Convert the format of data to a format that your in-house examiner is familiar with or is required.
(m) Attorney and litigation support technology services.
(n) Law enforcement services.
(o) Evidence recovery training and conducting of seminars.

11.3. International Organisation on Computer Evidence (IOCE)

The International Organisation on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime ivnestigation and other computer related forensic issues. Comprised of accredited government agencies involved in computer forensic investigation, IOCE identifies and discusses issues of interest to its constituents, facilitates the international dissemination of information, and develops recommendation for consideration by its member agencies. In addition to formulating computer evidence standards, IOCE develops communication service between member agencies and holds conferences geared towards the establishment of working relationships.

The international principles governed by IOCE for the standarised recovery of computer based evidence are governed by the following attributes :

(a) Consistency with all legal systems.

(b) Allowance for the use of a common language.
(c) Durability.
(d) Ability to cross international boundaries.
(e) Ability to instill confidence in the integrity of evidence.
(f) Ability to all forensic evidence.
(g) Applicability at every level, including that of individual, agency and country.

There are certain principles which were presented and approved at the International Hi-Tech Crime and Forensic Conference in October 1999. These principles are as follows :

(a) After seizing digital evidence, actions taken should not change that evidence.
(b) When it is necessary for a person to access original digital evidence, that person must be forensically competent.
(c) All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved, and available for review.
(d) An individual is responsible for all actions taken with respect to digital evidences while the digital evidence is in their possession.
(e) Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

There were certain other items also recommended by IOCE for discussion and facilitation. These items were :

(a) Forensic competency and the need to generate agreement on international accreditation and the validation of tools, techniques and training.
(b) Issues relating to practices and procedures for the examination of digital evidence.
(c) The sharing of information relating to hi-tech crime and forensic computing, such as events, tools and techniques.

11.4. OECD Initiatives

Organisation for Economic Cooperation and Development (OECD) was set up in 1983 in Paris for initiating an international effort in harmosing the legal responses towards cyber crimes.[2]

OECD in the international conference discussed computer related crime and the need for changes in the penal codes of the member countries. OECD recommended member countries to bring in necessary changes in their penal legislation to cover certain types of cyber crimes.

OECD framed guidelines to provide a foundation on the basis of which the countries and the private sector working separately as well as severally may form a concrete frameworks towards the security of information systems. The aims and objectives of these guidelines were :

(a) To promote mutual cooperation between the public and private sectors in the development and implementation of such measures, practices and procedures.
(b) To foster confidence in information systems and the manner in which they are produced and used.
(c) To facilitate development and utility of information systems, nationally and internationally.
(d) To promote intenation cooperation in achieving security of information systems.

The OECD Guidelines are based on the following nine principles :

(a) Principles of Accountability : The owners, providers and the users of information system and other beneficiaries must have an explict responsibility and accountability.

(b) Principle of Awareness : The user and other concerned parties must have adequate knowledge of security system and related measures, practice and procedures so that they may have appropriate steps for security of their information system.

(c) Principle of Ethics : The rights, liberties and legitimate interests of others should be respected properly by security system provider of such information system.

(d) Principles of Multidisciplinary : All the relevant aspects including technical, administrative, organisational, operational, commercial, educational, legal, etc., should be taken into consideration in course of measures, practices and procedures for the security of information system.

(e) Principle of Proportionality : The costs, security levels, measures, practices and procedures of information system must

be appropriate and proportionate to the value of and degree of reliance on the information system.

(f) Principle of Integration : There must be adequate coordination in the measures, practices and procedures in the security systems so that other measures, practices and procedures of the organisation must function in the manner of coherent system.

(g) Principle of Timeliness : Public as well as private at the national and international levels should act in a timely and coordinated manner in order to prevent and to respond to the branches of security of information system.

(h) Principles of Reassessment : The information system and the requirement of their security vary from time to time and therefore the security of information system must be reassessed periodically.

(i) Principle of Democracy : The information system and its security should be compatible with its proper and legitimate use and flow of data and information in a democratic society.

The Council of OECD adopted these guidelines in 1980 as a recommendation to its member countries and the main objective of the guideliness was to ensure data quality, collection limitation, purpose specification, use limitation, security safeguards, openness, individual participation and accountability in the information systems all over the world.

11.5. Efforts of G-7 and G-8 Groups

The G-8 Expert Group was established by G-7 countries, Russia and the European Union in 1996 with objective to check the misuse of International Data Networks.[3] The group comprised several technical and legal experts of the member countries in the field of International Communication Networks. The group prepared and presented a comprehensive report in December, 1997. The expert group suggested the following legal measures :

(a) Strengthening International mechanism by creating a well defined set of minimum rules against cyber crimes.

(b) To create a legal system so that in all countries service provides must undertake responsible efforts to erase illegal contents on their servers when made aware of these contents. Thus should also ensure that the free

flow of data should not be hindered by attempts to block access to other servers and by holding access providers liable.

(c) To ensure countries adopting effective prosecution of cyber crimes, particularly in respect of search and seizure of computer systems and international networks.

(d) To install devices in international system for lifting anonymity in case of abuse, thereby requiring adequate legal safeguards for privacy rights.

(e) To develop an international information network and such other information system with object to ensure proper prosecution of illegal and harmful practices detected on the internet.

(f) To strengthen cooperation amongst the law enforcing agencies with special respect to urgent measures for freezing data in internation search and seizure procedures.

(g) All issues concerning jurisdiction must be categorically classified.

(h) To train and educate properly the law enforcing agencies invovled in the search, seizure and prosecution of cyber crimes.

11.6. Endeavours of Council of Europe

The Council of European Union has made several effective steps in harmonising the responses towards cyber crimes. It has appointed an expert committee which prepared the recommendation No. R (89) 9. The Council of European Union adopted and approved this resolution on 13th September, 1989. The resolution prepared a minimum list of offences necessary for a uniform criminal policy on legislacy concerning computer related cyber crimes and the council under its recommendation concerned also adopted certain resolutions on the problems of procedural law relating to information technology. Another committee of experts were appointed in 1997 by the Council of European Union for identification and definition of new crimes, jurisdictional rights and criminal liabilities due to communication through the internet. The representatives of various countries such U.S.A., Japan, Canada, South Africa, etc., were also present in the meeting along with the members of Council of Europe. The committee prepared a draft convention, which was adopted by the Ministers of Foreign affairs on November 8, 2001. The committee

comprising about 33 signatories at present, decided to invite more members to the convention.

The Council of Europe had adopted two conventions, first being the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data signed on 28th January, 1981 at Strasbourg and another convention was signed on November 23, 2001 at Budapest.

11.7. Measure of United Nations

The Secretary General of United Nations has prepared a report entitled "Proposals for Concerned International Action against Forms of Crime Identified in Milan Plan of Action", soon after the U.N. Congress on the Prevention of Crime and the Treatment of Offenders. Computer related crimes or cyber crimes were discussed in paragraphs 42-44 of the report. The U.N. Congress at its 13th plenary meeting adopted resolutions to intensify their efforts to fight against cyber crimes and, if necessary, with the following measures :

(a) Modernisation of national criminal laws and procedures in order to ensure that existing offences and laws concerning investigative powers and admissibility of evidnce in judicial proceedings.

(b) Modernisation of national criminal laws and procedures in order to ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings.

(c) To make provisions for the forefeiture or restitution of illegally acquired assets resulting from the commission of cyber crimes.

(d) Improvement of computer security and preventive measures, including for protection of privacy, the respect for human rights and fundamental freedoms and regulatory mechanisms pertaining to computer usage.

(e) To create awareness among the public, the judiciary and the law enforcing agencies to the problem and the importance of preventing computer-related crimes.

(f) Adoptation of adequate training measures for law enforcing agencies, judges and officials responsible for

the prevention, prosecution and adjudication of economic and computer based cyber crimes.

(g) Improvement of mutual cooperation with interested organisation for the sake of elaboration of rules of ethics in the use of comptuers and the teaching of these rules as a part of the curriculum and training in informatics.

(h) Adoptation of policies for the victims of cyber crimes which are consistent with the U.N. Declaration of Basic Principle of Justice for victims of crimes and abuse of power, which may include the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities.

Furthermore, the Eighth Congress also recommended through a resolution, that the Committee on Prevention and Control of Cyber Crimes should work for increasing international efforts in developing the comprehensive framework of guidelines and standards that would assist member states in dealing with cyber crimes and it should develop further research and analysis so that the states may deal effectively with the problems of computer-related crimes in future also.

11.8. Efforts of WTO

The aspects of intellectual property rights concerning trade and commerce have been specifically dealt with by the World Trade Organisation (WTO). General Agreement on Trade and Tariff (GATT) of WTO and Agreement on Trade Related Intellectual Property Rights (TRIPS) deal with piracy.[4] Section 5 of Article 61 of the TRIPS Agreement enables member states to provide criminal procedures for the sake of protecting the intellectual property rights. The provisions says, "Members shall provide for criminal procedures and penalties to be applied at least in case of wilful trade mark counterfeiting or copyright privacy on a commercial scale. Remedies available shall include imprisonment and/or monitary fines sufficient to provide a deterrant consistently with the level of penalties applied for crimes of corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements, the prominent use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of

infringement of intellectual property rights, in particular where they are committed wilfully and on commercial scale. The issues relating to the privacy with respect to the free flow of data was also discussed by the WTO. In the provisions of GATT Agreement, the WTO approved the privacy issue also as a justification for limiting international data flows.

11.9. Measures of World Intellectual Property Organisation (WIPO)

World Intellectual Property Organisation (WIPO) has also taken some measures for protection of intellectual property and control of privacy in cyber world. WIPO has published in 1987 model provisions for protection of computer programmes. Later on in 1983, a committee of experts of WIPO recommended that neither a special protection structure nor treaties should be considered at that time. A joint meeting of WIPO and UNESCO also held in Geneva in 1985 and the majority of the participant recommended for immediate steps for protection from cyber crimes.

Another conference of WIPO held in December 1990 adopted the WIPO Copyright Treaty (WCT) and the WIPO Performance and Phonograms Treaty (WPPT). These treaties contained several provisions for protection of copyrights throughout the world. The treaty envisaged for the contracting parties to provide legal remedies against the circumvention of technological measures for protection of data and author's rights.

11.10. Interpol and its Measures

Interpol is working hard to combat cyber crimes throughout the world. Interpol organised its first training-cum-seminar for investigators of cyber crimes in 1981.[5] Thereafter Interpol organised its International Conference on computer crimes in 1995, 1996, 1998, 2000 and 2003. The Interpol has made commendable effort by setting up "working parties" comprising group of experts at regional level at different parts of the world.

The "working parties" have made the compilation of the Computer Crime Manual (IICIM) in 1990 which is a useful practical guide for the experienced investigators. They have conducted several training programmes also to train the law enforcement agencies, specialising them in the internet investigation. They also

set up a rapid information exchange system having 24-hours response system.

11.11. Efforts in India

Any criminal activity that uses a computer either as an intrpumentality, target or a means for perpetuating further crimes which comes within the ambit of cyber crime. But due rapid and varied applications of computer or computerised instruments, the nature and scope of computer related crimes or cyber crimes are changing its nature and ambit rapidly. While the worldwide scenario on cyber crime looks bleak, the situation in India is also not any better. There are no concerete statistics but it is estimated that Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.[6]

Despite the Information Technology Act, 2000 there are still several grey areas that exist within the law. The IT Act, 2000 is, says experts, primarly meant to be a legislation to promote e-commerce. It is not very effective in dealing with several emerging cyber crimes like cyber harassment, defamation, stalking and so on. There is need of more dedicated legislation on cyber crime that can supplement the Indian Penal Code. A Mumbai based lawyer and cyber law specialist Prathmesh Popal says, "The IT Act, 2000 is not comprehensive enough and does not even define the term 'cyber crime'. In fact, the Act cites such acts under a separate Chapter XI entitled "offences", in which various crimes have been declared penal offences punishable with imprisonment or a fine.

The cases of spam, hacking, cyber stalking and e-mail traud are rampant and although many cyber crime cells have set up in major cities, most of the cases are remain unreported due to lack of awareness among people.

It is, however, satisfactory to note that despite these limitations, cyber crimes are being detected and culprits are being punished. In October 2002, the Delhi High Court restricted a person from selling a pirated Microsoft Software over an Internet auction site. A case was decided successfully at the Metropolitan Magistrate in New Delhi, involving an online cheating scame when the accused was charged with using a stolen card to buy products from a Sony India Pvt. Ltd. website.

The experts are of opinion that the law enforcing agencies in India are not well-equipped and oriented about cyber crimes yet. There is an immense need for training, and more cities need to have cyber crime cells. India need special tribunals headed by trained individuals to deal solely with cyber crimes, but with powers to levy heavier penalties in exceptional cases. Unless there is solid deterrance, believed experts, cyber crime will rise steeply. There is also need of IT-Say lawyers and judges, as well as training for government agencies and professionals in computer forensics. Above all, awareness is of utmost importance and the Accurrences of cyber crimes must be reported at once.

There are many cyber police stations set up at various cities and they are performing well. Karnataka has reported about ninety-two cases from October 2001 to March 2003.

Table 11(a)

Statistics of Karnataka's Cyber Crimes (October 2001 to March 2003)

Nature of Crimes	No. of Cases
1. Hacking	16
2. Sending obscence mails	07
3. Tampering of source	01
4. E-mail abuse	25
5. E-mail spoofing	09
6. E-mail threat	04
7. Sending obscence message over e-mails/SMS	02
8. Post defamatory profile on net	05
9. Missing persons	05
10. Others	05
11. Copyright Act	17
Total	92

According to K. Srikanta, Deputy Superintendent of Cyber Police Station, Karnataka, out of total ninety-two cases recorded so far, only twenty-four cases come under the IT Act and in eight cases they (police) have filed charge sheets in the courts. Srikanta is of opinion that since there is no any defined act in Indian Penal Code (IPC), which could cover cyber crimes, so it is necessary that

a separate law should be enacted. India is perhaps the first country that has legislated the misconduct done in cyber world as a crime. People must know the important features of IT Act, otherwise, ignorance of it may put them behind the bars.

Table 11(b)

IT Act a Glance

(Penal Provisions)

Section	Penalty/ Punishment	Maximum Penalties
53	Penalty for damage to computer system, computer network	Rs. one crore
44 (a)	Failure to furnish any document, return or report to the controller or the certifying authority	Rs. 1,50,000
44 (b)	Failure to file any returns or furnish any information, books or other document	Rs. 5,000
44 (c)	Failure to maintain books of account or record	Rs. 10,000
45	Contravention of any rule or regulation for which no penalty is separately provided.	Rs. 25,000
65	Tampering with computer source documents	Up to 3 years imprisonment and fine up to Rs. 2 laks or both
66	Hacking with computer system	up to 3 years and fine up to 1 lakh or both
67	Publishing of information which is obscene in electonic form	up to 10 year and fine up to Rs. 2 lakh or both
72	breach of confidentiality and privacy	up to two years and fine up to 1 lakh
73	Publishing digital signature certificate false in particulars	up to 2 years imprisonment and fine up to Rs. 1 lakh

Police personnel are of opinion that "steganography" (sending message behind a picture) is a new challenge before police authority as sophisticated terrorists are using this method. Without the source Code, it is difficult to decode the message behind the picture and moreover the police don't have that kind of software to help them tracing the message. M.R. Devappa, Director of Prosecution in Karnataka, says "accused are on scooter but we are still riding bicycle".

11.12 Need of International Assstance and Appropriate Amendments

The impact of cyber crimes are global and, therefore, prevention and detection of such crimes involve international investigation. In view of cyber crimes being international crimes, the Information Technology Act, 2000 has extended its jurisdiction to all those acts or conducts, irrespective of the offender's nationality and location at the time of commission of offence, provided the act or conduct constituting the offence or contravention under the Act involves a computer, computer system or computer network. The Act does not deal with provisions enabling investigating officers making search and seizure of evidence from a system located at another country's jurisdiction. It is also a problem for the investigators how to obtain the presence of the accused residing in a foreign country.

In absence of such provisions in IT Act, we may rely upon the provisions of Criminal Procedure Code (Cr.P.C.) for dealing with the situations involving traditional crimes. Cr.P.C. contains provisions for reciprocal arrangements by Central Government with other countries through treaties or otherwise, for mutual assistance in the various matters like issue of processes (sec. Cr.P.C., 205), securing transfer of persons (Sec. 105 Cr.P.C.), and assistance in attachment of property or forfeiture of property (Sec. 82 Cr.P.C.), etc. Such reciprocal assistance made through "Letter rogatory", but this procedure is not very effective and proper in the cases of cyber crimes because speed is the essence of success.

The provisions of extradition an envisaged in Article 24 of the "European Convention on Cyber Crimes" must be effectively implemented which contain provisios for extradition of criminals involved in criminal offence provided such acts are punishable under the laws of both parties. This is very essential as in

prosecuting cyber criminals, it is essential to keep criminal to stand in trial.

Cyber laws in India, however, will soon be brought at par with global standard and made foolproof.[7] The group of law firms in India, U.S. and U.K.—commissioned by tech industry apex body NASSCOM to take a close look at the cyber regulation in all three countries and the kind of data security violations reported—has submitted its recommendations. The objective of the exercise was to ascertain to what extend Indian cyber laws provided protection against cyber violations. The team of law experts has identified some new areas in our cyber laws. The Ministry of Information Technology and Law are working towards making some amendments to the law so that all legal loose-ends are tied up properly.

11.13. U.S. Laws on Cyber Crimes

(a) Child Pornography Prevention Act : The internet provides ready access to a wide range of sexual contents, both legal and illegal. It is a crime to generate and distribute sexual images of children over the internet. This includes transmitting images of adults that have been modified to resemble children. Criminal liability includes a fine, as much as 30 years in prison, and forfeiture of the property used to transmit the illegal materials. (18 USC $ 2252 A, 2253). The U.S. Supreme Court has not ruled on the constitutionality of this law.

(b) Computer Fraud and Abuse Act : Accessing certain public or private computer systems without authorisation ("hacking" or "cracking") or in excess of one's authorisation is likely punishable as a crime. Computer systems of financial institutions and the U.S. Government receive special attention. This includes accessing the systems data, transmitting information to the system for the purpose of extortion. The U.S. Secret Service investigates these crimes, and prosecution can result in fines and up to 20 years in prison. (18 UCS § 1030). Initially, one court held that prosecution for copyright infringement that does not result in a financial gain to the defendant, and thus not subject to the Copyright Act, is also not available under the Computer Fraud and Abuse Act *U.S. Vs. LaMacchia,* 871 F Supp 535 (D Mass 1994). Congress responded to that "loophole" by amending the Copyright Act in 1997.

(c) Copyright Infringement : The reproduction and transmission of copyrighted materials, especially software, is greatly facilitated by the internet. Any person who wilfully infringes a copyright by reproducing or distributing the copyrighted materials by electronic means can face a fine and from one to six years in prison. (18 USC § 2319). Before 1997 the government had to show that the defendant realised a commercial or financial gain from the copyright infringement. See U.S. Vs. LaMacchia, 871 F Supp 535 (D Mass 1994). Congress amended the Copyright Act in 1997 to allow prosecution for reproducing or distributing copyrighted material over a certain market value, regardless of whether the defendant realised a commercial or financial gain.

(d) Digital Millennium Copyright Act : A portion of the Digital Millennium Copyright Act (DMCA) establishes federal civil and criminal sanctions against those who circumvent digital locks. It also outlaws manufacture of circumvention devices. The DMCA protects owners of copyrights, without regard to whether those owners were the creators of the protected work.

(e) Electronic Communications Privacy Act : This 1896 Act criminalisies intercepting electronic communications and accessing or interrupting access to electronic storage devices. (18 USC §§ 2510-2521, 2701-2711.) This statute provides a remedy for victims of hackers and persons pirating electronic transmission such as satellite television signals. *United States Vs. Chick,* 61 F3d 682, 687-88 (9th Cir 1995). Possibly the most notable aspect of this statute is its provisions alowing law enforcement agencies to employ electronic surveillance techniques when investigating investigating computer crimes. Although those provisions facilitate law enforcement activities, they also raise questions about the privacy of electronic communications.

(f) Mail and Wire Fraud : Transmitting by wire (*i.e.*, the Internet) "any writings, signs, signals, pictures, or sounds" for fraudulent purpose is subject to fine and up to 5 years in prison or, in the case of fraud affecting a financial institution, a fine of not more than $1,000,000 and 30 years in prison. (18 UCS § 1343.) Federal district courts have split on whether wire fraud statutes reach copyrighted materials. See, *e.g., U.S. Vs. Wang,* 898 F Supp 758, 759 (D Colo 1995); *U.S. Vs. LaMacchia,* 871 F Supp 535, 540-44 (D Mass 1994).

(g) Telecommunications Act : Title V of the Telecommunications Act (better known as the Communications Decency Act) was recently invalidated by the U.S. Supreme Court in *Reno Vs. American Civil Liberties Union.* The Court found that the Act's restrictions on "indecent" telecommunications violated the First Amendment of the U.S. Constitution. The Court, also on First Amendment grounds, invalidated the portion of the Act that criminalised "patently offensive" telecommunications to minors. Still valid, however, is that any person who knowingly transports "obsence" materials in interstate or foreign commerce via an interactive computer service "shall be fined under this title or imprisoned not more than five years, or both". (18 USC § 1465.)

11.14. U.S. Case-law on Cyber Crimes : Evidences and Related Issues

• ***Discovery of Electronic Evidence Allowable***

Adams Vs. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972) : Discovery of computer tapes if proper.

Anti-Monopoly, Inc. Vs. Hasbro, Inc., 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355 (S.D.N.Y. 1995)

Armstrong Vs. Executive Office of the President, 821 F. Supp. 761, 773 (D.D.C. 1993) : This case involves a challenge to the government's plans to dispose of electronic mail and word processing records of Reagan, Bush and Clinton White House officials at the end of each administration. In an August 1993 decision, the Federal Circuit Court for the District of Columbia Circuit ruled that electronic mail and word processing files must be managed as government records and sent the case back to the district court to determine whether the government's removal of the records at the end of the Bush Administration warranted sanctions for contempt of court.

Armstrong Vs. Executive Office of the President, 1 F. 3rd 1274 (D.C. Cir. 1993) : Government e-mail is covered as a record under the Federal Records Act; electronic version of e-mail must be maintained and produced.

Ball Vs. State of New York, 101 Misc. 2nd 554, 421 N.Y.S. 2d 328 (Ct. Cl. 1979) : State had to produce information contained on computer tape.

Bills Vs. Kennecott, 108 F.R.D. 459, 462 (D. Utah 1985).

City of Cleveland Vs. Cleveland Electric Illuminating Co., 538 F. Supp. 1257 (N.D. Ohio 1980) : Testifying expert's computer data and calculations discoverable.

Daewoo Electronics Co. Vs. United States, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986) : The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship.

Easley, McCaleb and Associates, Inc. Vs. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994) : Plaintiff's expert allowed to recover deleted files on defendant's hard drive.

First Technology Safety Systems, Inc. Vs. Depinet, 11 F. 3d 641 (6th Cir. 1993) : Trial court can issue *ex parte* electronic evidence seizure order.

Gates Rubber Co. Vs. Bando Chemical Industries, Ltd., 167 F.R.D. 90, 112 (D. Colo., 1996) : Site inspection and evidence preservation order. "Expert" criticised for procedures. A party has "a duty to utilise the method which would yield the most complete and accurate results."

Pearl Brewing Co. Vs. Joseph Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976) : Entire system documentation required to be produced.

PHE, Inc. Vs. Department of Justice, 139 F.R.D. 249, 257 (D.D.C. 1991) : Objection to discovery being burdensome denied.

Pink Vs. Oregon State Board of Higher Education, 816 F. 2d 458 (C.A. 9, 1987) : Tapes of faculty data were business records and useful for statistical analysis by experts.

Playboy Enterprises, inc. Vs. Terry Welles, 60 F. Supp 2 1050; 1999 U.S. Dist. LEXIS 12895 (S.D. Cal. 1999) : Court can appoint neutral expert to recover deleted e-mail.

Quotron Vs. Automatic Data Processing Inc., 141 F.R.D. : *Ex parte* order granted for conducting raid in software piracy case.

R.J. Reynolds, et al Vs. Minnesota, et al, U.S. Court Docket number 95-1611, cert. Denied May 28, 1996 : Reynolds compelled to turn over their litigation support database.

Santiago Vs. Miles, 121 F.R.D. 636, 640 (W.D N.Y. 1998) : "A

request for raw information in computer banks is proper and the information is obtainable under the discovery rules."

Seattle Audubon Society Vs. Lyons, 871 F. Supp. 1291 (W.D. Wash. 1994)

Simon Property Group Vs. mySimon, Inc., 2000 WL 963035 (S.D. Ind) : The court granted Simon Property's motion to produce electronic version of documents and make certain computers available for inspection. The court said that computer records are documents and discoverable under R. 34.

Williams Vs. E.I. du Pont de Nemours and Co., 119 F.R.D. 648 (W.D. Ky. 1987) : DuPont provided plaintiff with substantial employment data. Plaintiff created a database from the employment data. Court ruled the plaintiff had to provide the database to DuPont.

• ***Discovery of Electronic Evidence Denied***

Fennell Vs. First Step Design, Ltd., 83 F. 3rd 526 (1st Cir. 1996): Plaintiff's electronic discovery request was denied by Court, as plaintiff did not establish a "particularised likelihood of discovering appropriate information".

Hoffmann Vs. United Telecommunications, Inc., 117 F.R.D. 436 (D. Kan 1987) : Work-product doctrine protected discovery of computer file.

IBM Peripherals EDP Devices Antitrust Litigation, MDL # 163-RM (ND Cal Feb. 10, 1975) : Work-product material not discoverable.

International Business Machines Vs. Comdisco, Inc., 91-C-67-194, 1992 Del. Super LEXIS 67 March 11, 1992 : E-mail between client and attorney privileged.

Lawyers Title Ins. Co. Vs. U.S.F. & G., 122 F.R.D. 567 (N.D. Cal. 1988) : Wholesale electronic discovery not allowed unless shown that it would lead to material not previously produced.

Leeson Vs. State Farm Mutual Automobile Insurance Company, 190 III. App. 3rd 359, 546 NW2d 782, (1989, 1st Division) : Production of overly burdensome electronic discovery not required.

Munoz-Santana Vs. U.S. Immigration and Naturalisation Service, 742 F. 2d 561 (C.A. 9, 1984) : Expensive and substantial improvements to computer system necessary to retrieve data in format requested by plaintiff would not be required.

Strausser Vs. Yalamachi, 669 So. 2d 1142, 1144-45 (Fla. App. 1996) : Discovery request denied. Court determined the likelihood of recovering information was very small. Further, the system contained confidential patient records. The appeals court ruled that the request was overbroad.

U.S. Vs. Kupka, 57 F. 3rd 1078 (C.A. 9, California 1995) : Access to FBI computer system denied for failure to show nexus with.

- ***Duty to Preserve***

Dodge, Warren and Peters Ins. Services, Inc. Vs. James W. Riley, et.al., 105 Cal App. 4th 1414 (Cal. App. 4th District 2003): Defendants were former employees of plaintiff company. Before leaving to start their own firm, the employees copied documents from the company's computer systems. The company then terminated the employees and filed suit for misappropriation of trade secrets. The defendants appealed a preliminary injunction issued by the lower court preventing them from destroying potentially discoverable evidence on their computer systems. The appeals court refused to overturn the decision, finding that there was not an adequate remedy at law to protect plaintiff.

Proctor and Gamble Co. Vs. Haugen, 179 F.R.D. 622 (D. Utah 1998), aff'd in part and rev' d in part, 222 F. 3d 1262 (10th Cir. 2000): Duty to preserve exists independently of a court order.

Now Vs. Cuomo, 1998 WL 395320 (S.D.N.Y., decided July 14, 1998) : Duty to preserve arises at least with service of the complaint and counsel has a duty to advise client of pending litigation and the requirement to preserve potentially relevant evidence.

United States Vs. Smithfield Foods, Inc., 972 F. Supp. 338 (E.D. Va. 1997) : Producing party had obligation to preserve records once it was on notice of government's investigation.

Turner Vs. Hudson Transit Lines, Inc., 142 F.R.D. 68 (S.D.N.Y. 1991) : Duty to preserve what party knows or reasonably should know is relevant to the action or reasonably calculated to lead to discovery of admissible evidence, and the duty arises once party has notice of the relevance of the evidence. Notice will arise when the complaint filed or prior to the filing of the complaint when the party is on notice that litigation is likely to be filed.

National Ass'n of Radiation Survivors Vs. Turnage, 115 F.R.D. 543 (N.D. Cal. 1987) : Organisation was on notice of the allegations in the lawsuit and the discovery requests, and it is not a defence that particular employees in possession of the records were uninformed.

Thompson Vs. General Nutrition Co., 593 F. Supp. 1443 (C.D. Cal. 1984) : Computer and hard copy records destroyed by GNC after litigation started. Counsel has duty to preserve what counsel knows, or reasonably should know is : (1) relevant to the action, (2) reasonably likely to lead to discovery of admissible evidence; (3) reasonably likely to be requested during discovery; or (4) subject to pending discovery request. Default judgement and attorney's fees and costs awarded.

Bowmar Instrument Corp Vs. Texas Instruments, 1977 U.S. Dist. LEXIS 16078 (N.D. Ind., decided Mary 2, 1977) : Duty to preserve relevant evidence arises before a court order is issued and arises when party has knowledge, or should have known, of an impending lawsuit.

Applied Telematics, Inc. Vs. Sprint Communications Co., 1996 U.S. Dist, LEXIS 14053 (E.D. Pa., decided September 17, 1966) : Duty to preserve includes backup tapes prepared as part of disaster recovery, and normal backup and recycling of backup tapes should have been suspended during litigation.

Linnen Vs. A.H. Robins Co., 1999 Mass. Super. LEXIS 240 (Superior Court, decided June 15, 1999) : Party has obligation to preserve evidence, and even though hard copy of documents had been produced, the duty to preserve included backup tapes.

• ***Sanctions for Failing to Produce Electronic Evidence***

ABC Home Health Services, Inc. Vs. International Business Machines Corp., 158 F.R.D. 180 (S.D. Ga. 1994) : Defendant sanctioned for failing to maintain electronic evidence.

American Banker Insurance Co. Vs. Caruth, 786 S.W. 2d 427 Texas Ct. App. 1990 and 430 : Default judgement entered against defendant who twice failed to produce electronic evidence.

Computer Associates International Vs. American Fundware, Inc., 133 F.R.D. (D. Colo. 1990) : Defendant sanctioned for failing to maintain electronic evidence.

Crown Life Insurance Company Vs. Kerry P. Craig, US Court of

Appeals, 7th Circuit # 92-3180 : Craig submitted R. 34 document requests. The court ordered Crown to produce all the relevant documents. At trial, witnesses confirmed that the raw data requested by Craig and ordered by the court to be produced existed and that Crown's witnesses had used the data in preparing Crown's defence. The trial court sanctioned Crown for not producing the electronic data by barring testimony about the calculation of commissions and industry standards, which permitted Craig to recover the estimated future value of his commissions. On appeal, the 7th Circuit rejected Crown's argument that Craig requested documents, and did not specify raw data, i.e., the electronic data, was to be produced. The 7th Circuit held that computer data falls within "documents" under R. 34.

Illinois Tool Works, Inc. Vs. Metro Mark Products, Ltd., 43 F. Supp. 2d 951 (N.D. III. 1999) : A few days after the trial court issued an order requiring Metro Mark to preserve the integrity of all computers without spoliation, the key computer, which had functioned properly before the issuance of the court order, suddenly stopped functioning properly. Illions Tool Works sought sanctions. The court rejected "as totally unconvincing" Metro Mark's argument that it did not produce the electronic documents earlier because it did not understand that "documents" included both the hard copy and electronic version. Sanctions were imposed.

Lauren Corp Vs. Century Geophysical Corp., 1998 Colo. App. LEXIS 12 (No. 96CA0554, Jan. 22, 1998) : Sanctions imposed for failing to preserve requested electronic evidence.

Linnen Vs. A.H. Robins Co. Inc., 10 Mass. L. Rptr. 189 (1999): Court acknowledges significant expense in restoring backup tapes, but orders restoration reasoning that such is a risk undertaken by companies choosing electronic storage media.

National Association of Radiation Survivors Vs. Turnage, 115 F.R.D. 543 (N.D. Cal. 1987) : Sanctions imposed for allowing alteration and destruction of electronic evidence.

Prudential Ins. Co. of America Sales Practices Litigation, 169 F.R.D. 598 (1997) : Sanctions imposed for failing to preserve requested electronic evidence.

Shaw Vs. Hughes Aircraft, Orange Country Superior Court (1996):

Sanctions imposed for failing to preserve requested electronic evidence.

Wm. T. Thompson Co. Vs. General Nutrition Corp., 593 F. Supp. 1443 (1984) : Sanctions imposed for failing to preserve requested electronic evidence.

- ***Form of Electronic Production***

Adams Vs. Dan River Mill, Inc. 54 F.R.D. 220 (W.D. Va. 1972): Computer file must be produced in addition to the printout.

Greyhound Computer Corp., Inc Vs. IBM 3 Computer L. Serv. Rep. 138, 139 (D. Minn. 1971) : Material must be produced in a "reasonably usable form".

In re Air Crash Disaster, 130 F.R.D. 634 (E.D. Mich. 1989) : Computer file must be produced in addition to the printout.

State of New York and UDC-Love Canal Inc., Vs. Hooker Chemicals and Plastics Corp, Order, CIV-79-990 (W.D.N.Y. Nov. 30, 1989) : Material must be produced in a "rasonably usable form".

Minnesota Vs. Philip Morris Inc., Cl-94-8565 (Dist. Ct. Minn.): Printing out large amounts of data results in receiving party spending considerable time analyzing the information. Receiving the data in electronic form allows the receiving party to conduct necessary analysis.

National Union Electric Corp. Vs. Matsushita Electric Industrial Co., 494 F. Supp. 1257 (E.D. 1980) : Electronic evidence can be required to be produced in electronic form.

Williams Vs. Owens-Illinois, Inc., 665 F. 2d 918 (C.A. 9, 1982): Defendant required to process computer runs requested by plaintiff.

- ***Compelled Access to Hard Drive***

McCurdy Group, LLC Vs. American Biomedical Group, Inc., 2001 U.S. App. LEXIS 10570 (10th Cir. 2001) : Access to inspect hard drive was denied because the requesting party failed to demonstrate persuasive justification when other alternatives that do not create risk to attorney-client privilege and relevancy objections appear to be sufficient.

Sattar Vs. Motorola, Inc., 138 F. 3d 1164 (7th Cir. 1998) :The producing party was ordered to provide requesting party with

hard drive, software, or onsite access to producing party's computer system.

Fennell Vs. First Step Designs, Ltd., 83 F. 3d 526 (1st Cir. 1996): Access to hard drive was denied in light of the lack of probative justification after documents had been provided on disk.

In Re : Triton Energy Ltd., Securities Litig., 2002 US Dist. LEXIS 4326 (ED Tex., March 7, 2002) : During depositions, several outside directors testified that they had never been asked to produce documents relevant to the litigation.

Plaintiff sought access to defendant company's servers and hard drives to determine what, if any, e-mails and documents had been deleted during the pendency of the lawsuit. The court granted the motion and asked the parties to agree upon a neutral computer forensic expert, who will retrieve the information.

Ty, Inc. Vs. Le Clair, 2000 WL 1015936 (N.D. III., June 1, 2000): The court granted an emergency motion to compel access to computers on Ty, Inc.'s business premises.

Simon Property Group Vs. mySimon, Inc., 194, F.R.D. 639 (S.D. Ind. 2000) : The court granted Simon Property's motion to produce electronic version of documents and make certain computers available for inspection. The court said that computer records that have been deleted are documents and discovered under R 34, and it ordered the examination of the hard drive in question to recover the deleted files.

GTFM, Inc. Vs. Wal-Mart, 2000 U.S. Dist. LEXIS 3804 (S.D.N.Y., decided March 28, 2000) : A year after GTFM had requested electronic documents and Wal-Mart's counsel represented the electronic documents were no longer available, Wal-Mart's IT V.P. testified in deposition that at the time of the earlier request, the electronic data existed but by the time of his deposition, the data was no longer available. Court ordered Wal-Mart to permit GTFM to inspect computer and records on-site.

Playboy Enterprises, Inc. Vs. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) : In rejecting Welles' arguement against Playboy's accessing her hard drive, the court said that R. 34 covers electronic data compilations, such as e-mail, and ordered Welles to make her computer available for inspection.

Gates Rubber Co. Vs. Bando Chemical Industries, Ltd., 167 F.R.D. 90 (D.Colo. 1996).

Stasser Vs. Yalamanchi, 669 So. 2d 1142 (Ct. App.Fla. 1996): To access a computer, the requesting party must present evidence that purged data can be recovered. If access is ordered, the trial court has to establish protocols to protect privileged information and potential harm to producing party's data.

- ***Employee Email***

Blakey Vs. Continental Airlines (2000) 751 A. 2d 538 (NJ Sup. Ct.) : Employer potentially liable for employee's harassing e-mail.

Bourkey Vs. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993) : Employees had no reasonable expectation of privacy in their company e-mail.

Smyth Vs. Pillsbury Co., 1996 WL 32892 (E.D. Pa. 1/23/96 Weiner J.) : Employee had no reasonable expectation of privacy in company e-mail.

- ***Admissibility of Electronic Evidence***

7 ALR 4th 8, Admissibility of Computerised Records.

8 Federal Procedural forms Section 23 : 277.

12 Federal Procedural Forms Section 45 : 122.

16 AM JUR Proof of Facts Section 273.

32B AM JUR 2nd Federal Rules of Evidence Section 235.

Acierno Vs. New Caste County, 1997 U.S. Dist. LEXIS 11437, Robinson, J. (D. Del. May 28, 1997) : E-mail admissible.

Burleson Vs. Texas, 802 S.W. 2d 329 (Tx. App. 2d Dist. 1991): Computer generated report admissible.

Casey Vs. Zeneca Inc., 1995 U.S. Dist. LEXIS 5656, Schwartz, J. (De. Del. March 31, 1995) : E-mail admissible.

Hahnemann University Hospital Vs. Dudnick, 292 N.J. Super, 11 (App. Div. 1996) : Electronic evidence is generally reliable.

Harley Vs. McCoach, 928 F. Supp. 533 (E.D. Pa. 1996) : E-mail admissible.

Knox Vs. State of Indians, 93 F. 3d 1327 (7th Cir. 1996) : E-mail admissible.

Mesquite Vs. Moore, (1990 Texas App. Dallas) 800 SW2nd 617: Ordinary evidentiary rules apply to electronic evidence.

The Monotype Corporation, PLC Vs. International Typeface Corp., 41 F.R. Evid Serv. 86 (9th Cir. 1994) : E-mail message of non-party inadmissible—not a business record (Federal Rule 803 (6)).

National Union Electric Corp. Vs. Matsushita Electric industries Co., 494 F. Supp. 1257 : Copying a computer disk is equivalent to photocopying a paper document.

N.C. Electric Membership Corp. Vs. CP&L Co. 110 F.R.D. 511, 517 (M.D.N.C. 1986) : Internal, non-legal business e-mail not privileged.

Persons Vs. Jefferson Pilot Corp., 141 F.R.D. 408 (M.D.N.C. 1992) : Privilege lost when e-mail shared via the Internet with a third party.

People Vs. Holuwko, 109 III. 2d 187, 486 N.E. 2d 877 (1985): Computer printouts of telephone traces not hearsay; admissible.

QualityAuto Serv. Vs. Fiesta Lincoln-Mercury Dodge, Inc., No. 04-96-00967-CV, 1997 WL 563176 (Tex. App. Sept. 10, 1997) : Computer generated compilations of invoices qualify as business records.

Somerset Pharmaceuticals, Inc. Vs. Shalala, 1997 U.S. Dist. LEXIS 11461, Robinson, J. (D. Del. June 13, 1997) : E-mail admissible.

Stender Vs. Lucky Stores, Inc., 803 F. Supp. 259 (D.C.N.D., California, 1992) : Tapes from comptuerised payroll system considered to be authentic business records for expert to analyse.

Welsley College Vs. Pitts, 874 F. Supp. 375 (D. Del. 1997) : E-mail admissible.

U.S. Vs. Catabran, 836 F. 2d 453 (9th Cir. 1988) : Printouts from accounting software qualify as business records.

U.S. Vs. Kim, 595 F. 2d 755 (D.C. Cir. 1979) : "Critical factor in determining whether the document satisfied the 'business purpose' requirement lies in the reason that the message was prepared and sent, not the means by which it was transmitted."

- ***Costs***

In re Brand Name Prescription Drugs Antitust Litigation 1995 WL 360526 (N.D III.) : Defendant ordered to design e-mail retrieval

programme at its own expense; need for retrieval was foreseeable and cost resulted from defendant's choice of system.

Cabell Vs. Norton, 206 F.R.D. 27 (D.D.C. 2002) : After receiving a court order requiring them to restore backup tapes, defendants sought a protective order allowing them to produce the data in paper form. The court denied the defendants' request, which had been made twice before, and required them to pay plaintiffs' costs and fees incurred in responding.

Penk Vs. Oregon State Board of Education, 99 F.R.D. 504, 505 (D. Or. 1982) : Both sides share cost of updating database for trial.

Sattar Vs. Motorola, Inc., 138 F. 3rd 1164 (7th Cir. 1998) : Sattar appealed trial court's summary judgement dismissal, contending that the court abused its discretion in denying his motion to compel defendant to produce e-mails in a readable format. Trial court had gven the parties a number of options, including cost splitting. The Seventh Circuit called this "entirely reasonable".

Laura Zubulake Vs. UBS Warburg, LLC, et al, 2003 U.S. Dist. LEXIS 7939 (SDNY May 13, 2003) : The court found that Rowe test was incomplete and erroneously gave equal weight to all of the factors when certain ones should predominate. The court created a new seven factor test : (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources availability to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information. The court found the factors must be weighted in descending order of importance.

Byers Vs. Illinois State Police, 2002 WL 1264004 (ND III June 3, 2002) : In an employment discrimination suit, the court found that plaintiffs, who had sought to recover archieved e-mails from defendants, failed to establish that the search would uncover relevant information. The court required plaintiffs to pay the costs of the software needed to access the e-mails, and defendants were

required to pay the costs of reviewing the e-mails for relevance and privilege.

Rowe Entertainment Inc. Vs. The William Morris Agency, et al., 2002 US Dist LEXIS 488 (S.D.N.Y. 2002) : Court shifted costs of the production of e-mails and backup tapes to the requesting party. If the producing party wanted to review for privilege prior to turning docs over then they must shoulder this expense. In making its decision, the court looked at the following factors : total costs; the parties' ability to control costs; benefit to producing party; specificity of request; likelihood of successful search; availability from other sources; purpose of retention; and the parties' resources.

Murphy Oil USA Vs. Fluor Daniel Inc., 2002 US Dist LEXIS, 3196 (E.D. La 2002) : Using Rowe factors, court found that costs to retrieve e-mails from backup tapes should be shifted to the requesting party. However, the company was to bear the cost of culling pertinent e-mail from non-responsive e-mail and identifying privileged documents.

McPeek Vs. Ashcroft, et al., 2002 WL 929898 (D.D.C. 2001) : Court ordered defendants to restore the e-mails on backup tapes over a one-year period. The parties will then meet and argue whether the results and costs warrant further searches.

Bills Vs. Kennecott Corp., 108 F.R.D. 459 (D. Utah 1985) : Defendant recovered requested electronic documents and sought to shift costs. The court refused after looking at several factors : (1) is cost to recover "excessive" ? (2) is burden greater to producing party to requesting party ? (3) will producing party benefit ?

In Re : Brand Name Prescription Drugs Antitrust Litigation, 1995 US Dist LEXIS 8281 (ND III. June 1995) : Court refused to shift cost of producing defendant's e-mail ($50-70,000) because it found it found the costliness of discovery is a product of a computerised record keeping system.

Linnen Vs. AH Robins Company, Inc., et al., 1999 Mass. Super, LEXIS 240 (Superior Court, decided June 15, 1999) : Plaintiff demanded restoration of 100 backup tapes estimated to cost in excess of $1 million. The court refused to shift the costs, noting it was a risk taken by defendant when it decided to avail itself of computer technology.

References

1. file// H:/Articles/20-% 20 cyber % 20 crimes. htm.
2. Guidelines on the Protection of Privacy and Transborder, Flows of Personal Data, 1980, OPCD.
3. www.g7.utoronto.ca/crime/paris200.htm.
4. www.ifs.univie.ac.
5. MacManis, C.C., "Intellectual Property Protection and Emerging Computer Technology : Taking TRIPS on the Information Super Highway", V.L. Rav. 1997.
6. http://www.interpol.int/public/Technology/Crime/default.asp.
7. file : //H:\cyber/20 crime% 20 scene % 20 in % 20 India.htm.

12

Human Rights Perspectives in Cyber Crimes

Synopsis

12.1. Introduction

Human rights are those rights which belong to an individual as consequences of being a human being. They are based on elementary human needs. The recent advances in the field of information technologies is breaking down the barriers of what is called private and what is public. Every citizen, around the world, has right to maintain privacy. Various activities such as

forms of obscenity, expressing social or ethnic hatred through conversion or public forums, breaking of privacy of other individuals, etc., are under the cover of the law. But when these matters are discussed or carried out in the cyber space, they become both private as well as public. Various services, being provided on the cyber space such as internet chat, discussion group, news groups and other information gathering, disseminating services and communication services are both private as well as public and, therefore, are posing a dilemma to people as to how to deal with them. Their propagations are protected by the right of freedom of speech and expression. Any attempt to stop or cause hindrance to its propagation shall affect the right to freedom of speech and expression. Every citizen has right to maintain confidentiality and this right has been affected severely due to hacking and similar other computer crimes.

12.2. Ideological Aspects

Cyber space is in fact a world of its own and also a reservoir of information of various kinds. Knowledge is the power and the internet, of course is nowadays a resource of power. Cyber space has almost oceanic depth of knowledge and information. Many experts are of opinion that cyber space cannot be regulated by the states because they have no jurisdiction over it. Cyber space has its own individuality and position and therefore, the conventional rules do not apply to the alien territory.

The internet provides a vehicle for intra-gang communication as well as for deceiving the victims. Numerous operations in the field of trafficing in human beings, especially women and children, drug peddling, pornography and money laundering are being carried out all over the world with the help of internet. Financial institutions are the major target to the computer criminals. The areas of online banking is now much advanced. Bank are now able to attract more customers through online bankings. The emphasis is on making such access more and more customer friendly, but this comes with a price. There is feeling that many banks tend to underplay the simultaneous need for making this system more secure. This is out of sheer ignorance as well as a reluctance to make a heavy investment in IT security. The unhappy situation has been exploited by many crooks who do not hesitate to by skills in the market gadgets or well as human resources to

break into online banking system. According to a recent CSO magazine survey conducted in collaboration with the United States Secret Service and the Cyber Security Centre of the Carnegie Mellon University, electronic crime during 2003 accounted for a loss of $ 66 million.[1]

Customer negligence has also contributed to valuable information such as user ID and passwords falling into wrong hand. While major breakins have not been either frequent or well publicised, what is most appalling is that many banks have refused to let cyber investigators probe such breaches. This apathy is prompted by the fear that an admission of system vulnerability would result in the loss of customer confidence and could even lead to a run on the bank. Many are deterred also by the tortuous purpose of the criminal time of incidents are reported to the police. Another piece of criticism has been the enormous cost of many computer security products. Such negative feeling has engendered by the almost weekly arrival in the market of anti virus packages. Awidst many challenges, the problem that still remains to achieve a balance between the rights of the individual and the collective rights of the society in the cyber space.

12.3. Fundamental Rights and Civil Liberties

There are many private affairs being carried out on the internet. Many confidential private informations are also being preserved in the computers. Now a pertinent question is gripping in the minds of people that can the government restrict or affect the fundamental rights such as freedom of privacy, freedom of association, freedom of expression, freedom of political participation, etc., in the guise of regulating internet ?

It has undoubtedly became necessary for government and law enforcing agencies to monitor and keep a surveillance on the activities going on in the cyber space to ensure that criminal activities on the Net is detected and controlled. Such actions are necessary for the sake of detection and prevention of cyber crime even if it has to be done at the cost of affecting a bit the fundamental rights and civil liberties of citizens. But the only apprehension is that such power may be abused enforcing agencies. The laws relating to privacy by its has not been admitted under the Constitution of India but the rights of privacy is now implicit under the right to life on account of various judicial pronouncements.

12.4. Various Issues and Challenges

- *Freedom of Speech and Expression*

The fundamental right of speech and expression available to the human beings are positively affected by the cyber space which allows flow of information at less cost and highest speed and accuracy. There is general assumption that such rights should be free from the interferences of state.

Article 19 of the Universal Declaration of Human Rights provides that everyone has the right to freedom of opinion; and expression. This right includes to hold opinions without interferences and to seek, receive and impart information and ideas through any media and regardless of frontiers.[2]

Article 19 (2) of the International Convenant on Civil and Political Rights that "Everyone shall have the right to freedom of expression. That right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of fronties, either orally or in writing or in print in the form of art or through any other media of his choice."[3]

The citizens have a right to know about the activities of state, the instrumentalities, the departments and the agencies of the state in view of provisions under 'Freedom of Information Act, 2005.' The privilege of secrecy which existed in old times that the state is not bound to disclose the facts to the citizens or the state cannot be compelled by the citizens to disclose the facts, does not survive now to a great extent. Under Article 19 there exists the freedom of speech and expression. Freedom of speech is based on the Foundation freedom of right to know.[4] The state can impose and should impose reasonable restrictions in the rights where it affects the national security or any other matter affecting the nation's integrity. But the right is limited and particularly in the matter of sanitation and other allied matters, every citizen has a right to know how the state is functioning and why the state is withholding such information.[4]

- *Invasion of Privacy*

The right of privacy is now a part of fundamental rights enshrined under Article 19 (1) (a) of Constitution. The right of privacy is also a part to life and personal liberty enshrined under Article 21 of the Constitution.[5] The telephone tapping,

therefore, would offend Article 19 (1) (a) of the Constitution unless it comes within the grounds of restriction permissible under the Article.

The recent outcome of hi-tech cyber crimes in the cyber space have come up as a threat to individual's privacy. Enormous personal data about it in the cyber space and such data are under the threat of leakage and misuse. The exploitation of these confidential data for commercial and other purposes are also possible. Recent crimes of sending private and nude photographs of women by MMS in India is a similar type of invasion of privacy and abuse of cyber space. The leakage of U.K. citizens bank account by an employee of call centre has come up as a shock to all. Various law on protection of privacy, computer machine, surveillance and interception of telecommunication may provide some protection to the fundamental rights. Sec. 67 of I.T. Act provide protection to the right of privacy and prohibits publication or transmission of any material, but this provision has some shortcoming. The effectiveness of such law is open to be questioned in the wake of technologies development in the internet and economic power of those countries, which still fall out of the network of enforceable private laws.

• ***Unlawful Contents***

UNESCO has included in its programme the issue of illegal contents and has stated that action to counter illegal content which is harmful to specific groups and persons shall be part of its future plans and programmes. It has, therefore, taken significant initiatives against child pornography and paedophilia on the internet. It has been classified that such prevention programme cannot necessarily result into encroachment on freedom of expression.

Many government have already started taking initiatives against illegal contents. U.S. Government, for example, has enacted the U.S. Communication Decency Act, 1996 (CDA) to check criminalised online transmission of message and picture which are not obscene material but also lewd, lascivious, filthy or indecent material with intent to annoy, injure, insult, threat, or harass another person or if the recipient is under the age of 18 years.

Exploitation of children has become so ramppent that has taken the shape of serious problems. This problem has to be

tackled properly by the guardians of law. It cannot be left to the whims and fancies of perverted paedophiles. The players of cyber space must be educated properly and persuaded properly to make endeavour to minimise the problem.

- *Woman as a Victim*

Women are the worst victim of cyber crimes, the recent incident where a Delhi school student circulated a mobile video clip of two co-students having sex initiated a heated debate on right of privacy of women and even compelled authorities to ban mobile phones in educational institutions. The biggest fear are the IT and computer science students who are constantly making new discoveries on their cell phones. Such incident of pornographic MMS is repeatedly occurring at the various places of our country.

Another incident, where a landlord in Pune has installed a webcam in rented rooms occupied by college girls, has also aroused heated debate on laws relating to privacy of individuals, particularly women, in the country. Vyuerism in itself is not punishable under Indian laws, even if it is driven by spy cameras. If section 67 of the IT Act has to be invoked successfully, the police have to prove that the images captured by the accused were electronically published and it is very difficult to prove. Mohan Kulkarni, the accused of Pune incident, was charged under section 309 (word, gesture or act that insult the modesty of a woman) and section 294 (obscene act and songs) of Indian Penal Code and section 67 of I.T. Act, 2000. As against simple imprisonment up to one year under section 509 IPC, the IT Act, 2000 provides for imprisonment up to five years and fine of Rs. 1 lakh for a first conviction".

In the case of a second or subsequent conviction, the punishment escalates to ten years imprisonment and fine of Rs. two lakhs. Even in the case of seeking punishment under IPC sections 509 and 294, the conviction, a lot depends on the convincing arguments made by the public prosecutor and interpretation allowed by the judge.

The Supreme Court of India has recognised in 1964 that the right to privacy is implicit in the Constitution under Article 21, which specify the fundamental right to life. But the ruling applies only to the state and falls under the protection of Human Rights

Act, which led to the formation of the national and state human rights commissions. The concurrent crimes against women, therefore, has to be dealt under the present circumstances under the provisions of I.T. Act, 2000 and the Indecent Representation of Women (Prohibition) Act, 1987 and some sections of Indian Penal Code.

In the first ever incident of legal actions against cyber crimes in Muslim countries, a Saudi Court in Riyadh imprisoned three men to prison for orchestrating and filming the rape of teenaged girl in a case is which two Saudis has sexually assaulted and filmed with cellphones a 17-years old Nigerian girl. They distributed the video via the telephones and were caught by the police.[6]

- ***Collective and Individual Rights***

The human rights in cyber world cannot be articulated as individual right. It should be in fact recognised both as individual as well as collective rights. Cyber crimes occurring the vast panorama of cyber world affect people collectively. Cyber stal king, for example, is to have targeted mainly against women. Hate group and racists create propaganda against mass people and affect a particular large area of land. Even the crime of child pornography and exploitation of children on internet is affecting the innocent minds all over the world. The cyber community all around the world, therefore, must make a positive and collective effort to find a way to avoid such type of uncontrolled freedom of speech, so that "government and law enforcement does not get a chance to repose external censorship of cyber space."

- ***Invasion of Privacy by Unsolicited Calls***

In the present days of cyber world, no body's secrecy has remained safe. Every body's secrets, such bank accounts service record and even hospital records, are now safe and confidential. Now voices are being raised to ban unsolicited telemarking calls to consume as they are "an invasion of privacy and violation of the right to live a peaceful life". Even confidentiality in doctor-patient relationship is not guaranteed in India. Seeing medical care for AIDS, sexually transmitted infections can be risky as such confidentially be leaked any moment by doctor, nurse or computer operator of hospital.

A Chennai based medical professional was required to donate blood in the course of his duties. His blood test revealed that he was HIV positive. He was to have married soon, but the Chennai-based hospital informed his fiance's family of his HIV status without informing him first. When he sought damages from hospital for breach of confidentiality, the Apex Court rejected his plea upholding the hospital's right to breach of confidentiality.

- ***Breach of Confidentiality by Cell phone, Banking, Insurance Companies***

A Delhi-based person Mr. Shekhar Mishra, who had taken a home-loan last year, has been getting calls from a rival bank which informs him that his recent salary hike entitled him to a top-up loan at better rates. Such information, of course, was leaked by his banker. About such breach of confidentiality, the cell phone companies and banks claim that "dishonest lower-level employees" sell databanks for easy money. Since the right to privacy or confidentiality has not yet addressed under any law or statute in India, such breach is common at the cost of people's suffering. It is high time that Articles 19 and 21 of the Constitution of India, which safeguard the fundamental right to life and personal liberty, should be invoked, whether it be a matter of data protection, MMS or phone tapping.

It is also necessary that the provisions of Indian Penal Code and IT Act be amended and data-protection and privacy protection clauses be incorporated therein. Such unsolicited intervention is made at internet also and, therefore, appropriate legal measures should be taken to check such unsolicited advertisements calls on internet also.

12.5. Conclusion

The rapid developments in the field of cyber techniques are being proved to be both boon and bane for human beings. The abuse of technological devices are resulting into the serious threats to the people's human rights. The practical experience across the world shows that attempts to censure internet will have only limited success because of global nature of the net itself. A collective international measures, therefore, are necessary for checking abuse of cyber techniques and violation of human rights by the same.

References

1. *Frontline,* January 19, 2005.
2. Anand, V.K., *Human Rights,* Allahabad Law Agency, Faridabad, 2001, 897.
3. *Ibid.*
4. Bakshi, P.M., The Constitution of India, pp. 31-32.
5. L.K. Koolwal Vs. State of Rajasthan, AIR, 1988, Rajasthan, 268.
6. *The Times of India,* January 9, 2005.

Table 12.1

Protection of Human Rights in Indian Law : A Glance

Sl.No. (1)	Provisions (2)	Rights Concerning (3)
1.	Sections 49, 50, 55, 57, 75 and 76 of Criminal Procedure Code (Cr.P.C.)	Grant the citizens freedom from unjustified arrest, illegal detention, unnecessary restriction as well as the right to be informed of the grounds of detention and the right to consult lawyer of his choice.
2.	Sections 436, 437, 439 and Sections 50 (2) and 167 Cr.P.C.	Grants the citizen rights to secure bail if and when arrested.
3.	Section 309 Cr.P.C. and Article 21 of Constitution	Confers the right to fair and speedy investigation.
4.	Section 101 to 104 of the Indian Evidence Act, 1892	Presumes every citizen to be innocent until proved guilty.
5.	Articles 5 and 7 of Universal Declaration on Human Rights (UDHR) 2nd Covenant	Right of not to be a witness against oneself.
6.	Article 22 (1) of the Indian Constitution	Right to consult and to be defended by a legal practitioner of his choice.
7.	Article 31 of Indian Constitution	Right to privacy.
8.	Sections 93, 94, 97, 100 (4) to 108 and 165 of Cr.P.C.	Protection against arbitrary or unlawful arrest.

9.	Article 19 of Constitution	Foot-path trading, Pension, Right to livelihood.
10.	Article 20 of Constitution	Double Jeopardy.
11.	Article 21 of Constitution	Legal aid to poors, Right to education, hand cuffing, Right to public health, Right to privacy, speedy trial, Right to livelihood, Right to go abroad, Prisoner's right to send manuscript for publication, Right to live in clean atmosphere, etc., are also within fundamental rights.

13

Cyber Crimes : Precaution and Prevention

Synopsis

13.1. Introduction

Whole world is now increasingly dependent on computer and internet services. Almost all the social and economic activities have shifted to computers and internet including match-making, accounting, business, banking, cash disbursal, etc., when majority of human activities are being shifted to cyber space, than criminal relatives are naturally to shift to cyber space. We have to now gear up to face it and make devices to prevent it.

The cyber crimes are comparatively more serious due to the internet characteristic and network functioning. Its global nature

and scope of anonymity is an important encouraging factor of the cyber criminals. Criminals are able to use the technology to conduct their activities in much sophisticated manner with relative safety because they may operate even from their homes and continents away from the actual "scene of crime". The important factors, which facilitates the vulnerability of cyber crimes are—density of information and process in the network, comparatively easy accessibility to the system, vulnerability due to dependence on telecommunication systems and uncertainties of the complex logical processes.

We cannot tackle hi-tech cyber crimes in the traditional and concurrent ways. We have to make sophisticated innovative strategies and technologies to combat menace of cyber criminals. The e-commerce and e-banking are now major target to cyber offenders and they may result huge financial losses. It is high time that each of financial institutions must have a technological expert to keep a watch on their system.

13.2. Awareness and Law Reforms

Present experiences with cyber crimes are showing that the traditional laws, enforcement agencies and concurrent, preparedness are guide inadequate enough to deal with cyber crimes. Police offers are not properly trained to deal with the situation. The investigating agencies are also not well trained to collect, seize and preserve the evidences concerning cyber crimes. The Indian Information Technology Act, 2000, which is primarily meant to be a legislation to promote e-commerce, is not very effective in dealing with several emerging cyber crimes like cyber harassment, defamation, stalking and so on. The Mumbai-based lawyer and cyber law specialist Prathmesh Popat rightly says, "The IT Act 2000 is not comprehensive "enough and does not even define the term 'cyber crime'". In fact, the Act cites such acts under a separate Chapter XI entitled "offence", in which various crimes have been declared penal offences punishable with imprisonment or a fine but still there are several grey area that exist within the law.

The well-known proverb "prevention is better than cure" may come to our help in the present situation. The adequate people's awareness and law reforms should be adopted at the earliest to deal with the hi-tech crimes. In the wake of creating

public awareness against cyber crimes, an expert Mr. Shailesh Zarker suggests a few security tips[1] as follows :

(a) Avoid giving out any information about yourself in chat room.

(b) Children should never arrange face-to-face meetings or send their photographs online without informing their parents.

(c) Use the latest anti-virus software, operating system, web browsers and e-mail programmes.

(d) Check out the site your are doing business with thoroughly. Send credit card information only to secure sites.

(e) Use a security programme that gives you control over cookies that send information back to website. Letting all cookies in without monitoring them could be risky.

(f) If you own a website, watch traffic and put host-based intrusion detection devices on your servers. Monitor activity and look for any irregularities.

(g) Put in a firewell and develop your content off line.

(h) Make sure web servers running your public site are physically separate and individually protected from your internal corporate network.

(i) Protect your database. If your website serves up dynamic content from a database, consider putting that database behind a second interface on your firewell, with tighter access rules than the interface to your server.

(j) Back up your website after every update, so you can re-lauch it immediately in case of a malacious defacement.

Besides awareness and any matter should be reported immediately to the police, it is also important that the user must try and save any electronic information trail on their computers.

13.3. Improving Criminal Justice Administration

The law enforcement agencies, legal and judicial communities now require to develop new skill to combat with the challenges presented by compùter crimes. The growing sophistication of telecommunications systems and the high level of expertise of many systems operators complicate significantly the task of regulatory and legal interventions.[2] The ignorance of

sophisticated techniques among the law enforcing agencies and the familiarity with electronic complexity in the general population is contributing to the rapid increase in cyber crimes. It is, therefore, now urgent to educate these agencies about the complex computer techniques so as to make them competent in enforcing the law. Law enforcing agencies, legal and judicial communities need to develop minimum level of skills and expertise to understand the complexities of the computer networks and sophisticated telecommunication systems so as to effectively deal with their possible misuse and indulgence in criminal activities.

Gone are the days when the computer crimes were maintained limited to the economic activities and therefore, the law enforcing agencies were given the training to deal with the economic offences such as fraud, embezzlements, etc. But after advent of internet revolution all around the world gripping the entire population of the world, the cyber crimes have acquired several forms affecting vast areas and have reached all the forms of traditional crimes including women and drug trafficking, industrial, banking and military espionage, etc. Therefore, the training and awareness campaign cannot be limited to the level of any group of personnel on the law enforcing agencies but has to be extended to all organisations involved in cyber crimes prevention endeavours.

U.N. Manual on the prevention and control of computer related crimes have identified five areas in which appropriate training should be given to all the members of judicial administration and enforcement agencies. These areas are as follows :

(a) Knowledge of Difference between Civil Wrong and a Criminal Wrong : Since all forms of computer abuse may not constitute a criminal offence, it is essential that persons concerned must be able to differentiate between the civil wrongs and the criminal wrongs. The law enforcing agencies, therefore, must be trained properly as to which activity or abuse of computer shall amount to a civil wrong or constitute a criminal offence.

(b) Both Technology and Computer Trainings : Police must introduce compulsory computer training to all its officers involved in detection, investigation and prevention of cyber crimes. Such training should include both computer and technological trainings. In the lack of appropriate, technological and computer

trainings police personnel may commit serious error in the course of their duty. For example, Mumbai Police once raided a house for alleged cyber crime but seized only monitor and not the CPU (Central Processing Unit). The police officers, therefore, must have the adequate technical knowledge. All persons involved in both prosecution and judicial duties must have adequate technical knowledge to be able to perform the work of prosecution and adjudication properly.

(c) Ability to Preserve Evidence and Present it Before the Courts: The task of collection of evidence in the paperless transaction of cyber world have become a challenging job. It differs from the traditional forms of evidences. It is, therefore, now essential that the legal system of present day must change so that the investigators may be able to search, collect, maintain, preserve and present it before the courts in a fair and proper manner. It is necessary because only well skilled personnel can handle computer datas so that there may not be the risk of damaging or modifying the original data.

(d) Involvement of the International Nature of Problem : In order to deal with cyber crimes, the investigation must be able to understand and deal with international issues, including extradition, mutual assistance, concerned laws, etc. Due to the global nature of cyber crimes, the investigators are required to have fair knowledge of laws of evidence, criminal procedure and data protection of other legal, jurisdiction while pursuing international investigation regarding cyber crimes.

(e) Rights and Priviledges of Involved Parties : UN further envisages that there should be training programmes for the personnels involved in the cyber crimes' investigation and adjudication so that they may be aware towards the rights and the priviledges involved in the cyber crimes. UN also desires that the Criminal Justice Administration also must be sensitive towards this problem. This is necessary because the credibility of the enforcement agencies involved in various jurisdiction depends upon their equitable application of law. If aspect of human rights and privileges are taken into consideration, this gesture will help in winning confidence of the people in general in the administration and as a result the victims and others coming into the knowledge of cyber crimes shall come forward with information and cooperation.

13.4. Increasing International Cooperation

The harmonisation of criminal and cyber laws at international level and cooperation between countries are now very essential for tackling the problem of cyber crimes. The advent of internet has virtually broken the national boundaries and whole world has not turned into a global village. The efforts at the level of organisation like OECD, UN, Council of Europe, etc., are afoot for increasing international cooperation. The convention of European Council has taken resolution to increase international cooperation among member countries for the timely assistance to each other in preventing and detecting cyber crimes.

Some private organisations and universities have also come forward for strengthening international cooperation for the sake of checking cyber crimes. Stanford University, for example, has organised a conference on International cooperation to fight against terrorism and cyber crimes in December, 1999 and resolution was introduced in August, 2000.[3] The international organisations, such as Interpol, are also making efforts in the field. Interpol organised first training camp to train investigators of cyber crimes in 1981. Thereafter several seminars were organised in different parts of the world.

U.S. Attorney General in January, 2000 suggested state and local law enforcing agencies to adopt the following measures to:

(a) Establish a 24-hours cyber crimes point of contract network where law enforcing agencies belonging to federal, state and local law enforcing agencies may meet with each other to exchange their information. Their contact should be coordinated through a centralised "command centre".

(b) Create an online clearing house for sharing information to avoid duplication of effort and multiple investigation of the unlawful conduct in the cyber world.

(c) Organise conferences of all state and local cyber crime investigators annually or bi-annually for discussion on recent developments, sharing of cases, progresses, enforcement of networks, etc.

(d) Develop new additional policies and mechanism to increase international cooperation between world's law

enforcing agencies and investigators and to encourage coordination among them.

Cyber crime cannot be checked unless it is made an offence all over the world. We cannot control cyber crime in the situation when one country's laws declares it a criminal offence and another country's law do not. So, it is now necessary to establish global cooperation to solve the crime and to make possible the extradition of criminals for effective trial.

13.5. Curricular Endeavours and Checking Kids' Net Addiction

Children are one of the most easy victims of cyber crimes. The increasing obsession of children towards the internet chat and games is matter of serious concern. Media has highlighted many cases of obsessed internet gamers, some of whom have flunked out of school, committed suicide or murder. Internet cafes continue to thrive, with outlets in even the smallest and poorest of villages.

According to officials figures, China has the world's second largest online population, about 94 million, after the U.S.[4] and has also the largest number of kids having Net addiction. China is the first country to establish officially licensed clinic for internet addiction. Dr. Tao Ran of the clinic says about the children undergoing treatment here, "They are suffering from depression, nervousness, fear and unwillingness to interact with others, panic and agitation. They also have sleep disorders, the shakes and numbness in their hands." Further says, "All the children here have left school because they are playing games or in chat rooms everyday."[5]

Popular computer games for children having hidden sex trips are also producing adverse effects on their mind. For example, the latest version of a popular game called 'The Grand Theft Auto (GTA)' looks like any other action packed 3D animation fare in which the player goes on a mission down city lanes. The innocent user will play within the apparent boundaries of an imaginary city, modelled after Los Angles. But many young users all over the world, including India, are downloading a free patch (a set of software codes, usually created by a hacker) from the internet that suddenly gives access to hidden alley. Dr. Harish Shetty, a noted psychiatrist, says, "Parents do not know much about the games

that their children are playing. In fact, some parents gift such games. All that parents see on the children's computer monitor are stars, rockets and the moon. With a mouse click the children hide what they do not want the parents to see. I would advise the parents to trust their kids but keep their eye open."[6]

Although some games with explicit sexual content are clearly labelled "A", the games like the Grand Theft Auto does not come with such a warning, obviously because the creators intended to hide the sexual content.

The time has how come when the children and even adults should be given lessons about acceptable online behaviour so that internet may remain a safe and useful medium. There is also need to educate the people on the danger being posed by cyber crimes and how the people can reduce the dangers of cyber crimes. Thus, there is need to introduce safety measures in the curriculum of universities and colleges.

13.6. Role of Guardians

The parents and guardians have an important role to play in moulding the character and conduct of their children in the society. They can also play an important role in protecting children from the ill effects of cyber space. Since home is the first school, they may teach their children how to use internet and avoid the harmful sites with greater responsibility. The following are the some of the safety measures which guardians may adopt to protect their children from harmful effects of internet[7] :

(a) They should not give any kind of personal information. Such as residential address, school's home, telephone number, etc., in chat room or bulletin board.
(b) One should not leave photographs on websites.
(c) Children should not be allowed to face-to-face meeting with another computer users without guardian's permission.
(d) Guardians should keep an eye on the children's companions.
(e) Children should be encouraged to inform parents about any message received by them.
(f) Children should be asked not to respond to message which are obscene, suggestive, belligerent, threating.

(g) Computer should not be kept in children's bedroom and the online use of computer by them should be monitored.
(h) Guardians should know the online friends on their children as they know about their other friends.
(i) Parents should permit limited use of internet to their children.

There are many websites which provide appropriate guidelines for the parents and make available necessary software programmes for checking the children's access to improper materials. The school teachers and libraries may also provide appropriate guidance to the children.

13.7. Mobile Pornography : No Nearer Solution in Sight

Recent MMS clip of porn film Bollywoods heroine Mallika Sherawat in nude poses has hit the headlines of almost every newspapers. A six-minute video sex clip of a Sherawat lookalike with a foreigner has been burning up mobile phone in Mumbai. Such incidences of titillating MMS clip have been on rise—the alleged Rhea Sen Ashmit Patel clip, the alleged Kareena Kapoor-Shahid Kapur Kiss had started the trend, the Delhi School MMS Mobile porn is here to stay and the right to privacy is clearly the victim.

In the last few years, technology in the area of electronic communication has developed to such an extent that it is capable of being misused and abused. But there is no technological device nor there is specific legislation to deal with the abuse of electronic data which has been doctored. The Information Technology Act, 2000 is not really equipped to deal with the day-to-day problems of offensive electronic message.

According to the law, any form of electronic communication which tends to "outrage the immodesty" of a person infringes on personal or family relationships is an invasion of privacy. It is engraved as a fundamental right under Article 21 (right to life and personal liberty) of the Constitution, and every person is entitled to safeguard such privacy. The Supreme Court has held that the right to privacy is a part of fundamental right and held further that even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and when he likes.

However, the technological advances in the age of downloads

and hi-tech handsets have been so sweeping that the law-makers have evidently not reckoned with them.[8] For example, the case of Pune landlord who installed a camera in a toilet and caught his lady tenants in a compromising situation. And also in the case of BPO in Mumbai who captured two of its employees "making out" a loo. The BPO wanted to sack them but the duo, in turn, accused the company of violation of their right to privacy. The company refrained from taking any action.

The IT Act bans dissemination of obsence images and makes such action punishable by up to five years. It is cognisable but its implementation is far from satisfactory. For instance, Mallika Sherawat's lawyer has sought a police investigation into MMS under the IT Act. But police demanded the copy of MMS clip to proceed with. Police finds it difficult to establish the source and hence chance of conviction are hard to come by.

The number of MMS messages are now increasing very rapidly. Last new year's night, 60 million MMS greetings were passed. A billion message are sent every month.[9] At an average rate of one rupee per message, it is a considerable sum of earnings. Service providers are also planting porn messages. Now nearly 57 million persons have cell phones that allows MMS. That's why the issue of MMS pornography is increasing at alarming extent.

13.8. Self-regulation in Cyber Space

Self-regulation is also an important strategy, which is the strategy of adopting soft laws for self-regulation by the users and service providers of the internet. Such self-regulatory device is popularly known as "Netiquette", which are in fact gentlemen's agreement and can be very effective in calculating the proper behaviour amongst the Net users. Services providers may play an important role in developing and implementing properly these Netiquettes. They can make such regulations a part of their service contract with condition to that effect that any violation shall lead to discontinuouance of service. For example, the user guidelines of Sunrise Internet Service contains such type of conditions.

The Department of Justice and the Information Technology Association of America (ITAA) has initiated a joint campaign to educate and raise awareness of computer responsibility among

the users. They have also initiated a national compaign to educate and arouse consciousness of computer responsibility and to provide resources to empower concerned people. Such awareness programme should now be made a part of the schools and colleges' curricula to create awareness among cyber citizens.

13.9. Conclusion

The awareness and capacity building among cyber people and law enforcing agencies should be given the top priority. The role of parents and teachers in moulding the cyber behaviour of future generation should also be given adequate priority. Strict enforcement of cyber regulations should be ensured at all levels. The major focus should be given to the international efforts of mutual cooperation.

References

1. file : //:\Cyber/20 crimes % 20 scene in %20 India.htm.
2. UN, International Review of Criminal Policy—UN Manual on the Prevention and control of Computer Related Crimes.
3. http : cisac.stanford.edu.
4. *The Times of India*, July 3, 2005.
5. *Ibid.*
6. *Ibid.*, July 21, 2005.
7. *Ibid.*
8. *Ibid.*, July 14, 2005.
9. *Ibid.*, July 14, 2005.

"This page is Intentionally Left Blank"

Part-II

"This page is Intentionally Left Blank"

Appendix 1

The Information Technology Act, 2000

(21 of 2000)

[9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto;

Whereas the General Assembly of the United Nations by resolution A/RES/51/162, dated 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

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

And whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records;

Be it enacted by Parliament in the Fifty-first Year of the Republic of India as follows :

Chapter 1
Preliminary

1. Short title, extent, commencement and application--(1) This Act may be called the Information Technology Act, 2000.

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

(3) It shall come into force on such date[1] as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to :

[2][(a) a negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instrument Act, 1881 (26 of 1881);]

(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882);

(c) a trust as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1882);

(d) a Will as defined in clause (h) of section (2) of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called;

(e) any content for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2. Definitions—(1) In this Act, unless the context otherwise requires,—

---

1. Came into force in 17th October, 2000 *vide* G.S.R. 788 (E), dated 17th October, 2000.
2. Subs, by Act 55 of 2002, sec. 12, for clause "(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881)"; (w.e.f. 6-2-2003).

(a) "access", with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under sub-section (1) of section 46;

(d) "affixing digital signature", with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,—

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certification under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

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

(j) "computer network" means the interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

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

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer) printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) "electronic form", with reference to information, means

any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function" in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

(w) "intermediary", with respect to any particular electronic message, means any person who on behalf of another receives, stores or transmits that message or provides any service with respect to that message;

(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message; or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

(zh) "verify", in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

Chapter II

Digital Signature

3. Authentication of electronic records.—(1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another record.

Explanation—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Chapter III

Electronic Governance

4. Legal recognition of electronic records—Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signature—Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with

reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies—(1) Where any law provides for—

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner;

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

7. Retention of electronic records—(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record :

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette—Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette :

Provided that where any rule, regulation, order, by-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Section 6, 7 and 8 not to confer right to insist document should be accepted in electronic form—Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature—The Central Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

Chapter IV

Attribution, Acknowledgement and Despatch of Electronic Records

11. Attribution of electronic records—An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgement of receipt—(1) Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by—

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has been so received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no

acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record—(1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :

(a) if the addressee has designated a computer resource for the purpose of receiving computer electronic records,—

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipts occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despated at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section,—

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place

of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Chapter V

Secure Electronic Records and Secure Digital Signature

14. Secure electronic record—Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature—If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated,

then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure—The Central Government shall, for the purposes of this Act, prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including—

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference of their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

Chapter VI

Regulation of Certifying Authorities

17. Appointment of Controller and other officers—(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification, appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller—The Controller may perform all or any of the following functions, namely :

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authority should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisement that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities—(1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository—(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act .

(2) The Controller shall :

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government,

to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

21. Licence to issue Digital Signature Certificates—(1) Subject to the provisions of sub-section (2), any person may make an application to the Controller for a licence to issue Digital Signature Certificate.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfils such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall—

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence—(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by :

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence—An application for renewal of a licence shall be :

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees,

as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence—The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application :

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of licence—(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has :

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

[1][(c) failed to maintain the procedures and standards specified in section 30;]

(d) contravened any provisions of this Act, rule, regulation or order made thereunder;

revoke the licence :

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

1. Subs. vide S.O. 1015 (E), dated 19th September, 2002, for clause "(c) failed to maintain the standards specified under clause (b) of sub-section (2) of section 20"; (w.e.f. 19-9-2002).

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), suspend such licence pending the completion of any enquiry ordered by him :

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

26. Notice of suspension or revocation of licence—(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories :

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock :

Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

27. Power to delegate—The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this chapter.

28. Power to investigate contraventions—(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act,

1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data—(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures—Every Certifying Authority shall,—

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.—Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations or orders made thereunder.

32. Display of licence—Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence—(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after

such suspension or revocation surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure—(1) Every Certifying Authority shall disclose in the manner specified by regulations :

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Chapter VII

Digital Signature Certificate

35. Certifying authority to issue Digital Signature Certificate—(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement, containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application :

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that :

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant :

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate—A Certifying Authority while issuing a Digital Signature Certificate shall certify that :

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations in clauses (a) to (d).

37. Suspension of Digital Signature Certificate—(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate :

(a) on receipt of a request to that effect from—

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber.

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate : (1) A Certifying Authority may revoke a Digital Signature Certificate issued by it:

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that :

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Comments

A Digital Signature Certificate issued by a Certifying Authority can be revoked if the subscriber or any person authorised by him makes a request to that effect; or upon the death of the subscriber; or upon the dissolution of the firm or company where the subscriber is a firm or a company. Certifying Authority can also revoke a Digital Signature Certificate which has been issued by it if it is of opinion that : (i) a material fact represented in the Digital Signature Certificate is false or has been concealed, (ii) a requirement for issuance of the Digital Signature Certificate was not satisfied, (iii) the Certifying Authority's private key or security system was comprised in a manner materially affecting the Digital Signature Certificate's reliability, (iv) the subscriber has been declared insolvent or where a subscriber is a firm or a company which has been dissolved wound-up or otherwise ceased to exist.

39. Notice of suspension or revocation : (1) Where a Digital Signature Certificate is suspended or revoked under section 37 or

section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

Chapter VIII

Duties of Subscribes

40. Generating key pair : Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, [1][***] the subscriber shall generate[2] [that key] pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate—(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate.

(a) to one or more persons;

(b) in a repository; or

otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

---

1. The word "then" omitted by wide S.O. 1015 (E), dated 19th September, 2002 (w.e.f. 19-9-2002).
2. Subs by S.O. 1015 (E), dated 19th September, 2002, for "the key" (w.e.f. 19-9-2002).

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key—(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure [1][***].

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation—For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Chapter IX

Penalties and Adjudication

43. Penalty for damage to computer, computer system, etc.—If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network—

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminent or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

1. The words, "to a person not authorised to affix the digital signature of the subscriber" omitted by S.O. 1015 (E), dated 19th September, 2002 (w.e.f. 19-92002).

(e) disrupts or causes disruption of any computer, computer system or computer networks;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

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

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

Explanation—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network.

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

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction in executed or some other event takes place in that computer resource;

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

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

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

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

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

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

Comments

Any person who contravenes any rules or regulations made under this Act, he is liable to pay a compensation up to twenty-five thousand rupees to the person affected by such contravention.

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

(2) The adjudicating officer shall, after giving the person

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

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

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

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

(a) all proceedings before it shall be deemed to be judicial proceedings within the meanings of sections 193 and 228 of the Indian Penal Code (45 of 1860);

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

47. Factors to be taken into account by the adjudicating officer—While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely—

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

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

(c) the repetitive nature of the default.

Chapter X

The Cyber Regulations Appellate Tribunal

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

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

49. Composition of Cyber Appellate Tribunal—A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

50. Qualification for appointment as Presiding Officer of the Cyber Appellate Tribunal—A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he—

(a) is, or has been, or is qualified to be, a Judge of a High Court; or

(b) is, or has been, a member of the Indian Legal Service and is holding or has held a post in Grade 1 of that Service for at least three years.

51. Term of office—The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office until he attains the age of sixty-five years whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer—The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed.

53. Filling up of vacancies—If, for reason other than temporary absence, any vacancy ocurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal—(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office :

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office

sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not he removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, be rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings—No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal—(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal—(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed :

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal— (1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1905 (5 of 1908), while trying a suit, in respect of the following matters, namely :

(a) summoning and enforcing the attendance of any person and examining him on oath;

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

(c) receiving evidence on affidavits;

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

(e) reviewing its decisions;

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

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of section 193 and 228, and for the purposes of section 196 of the Indian Penal Code (45 of 1860) and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

59. Right to legal representation—The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation—The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction—No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court—Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order :

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions—(1) Any contravention under this [Act] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify :

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation—For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty—A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

Chapter XI

Offences

65. Tampering with computer source documents—Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment 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 programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Comments

Any person who knowingly or intentionally conceals, destroys code or alters or causes another to conceal, destroy, or alter any computer source used for a computer, computer programme, computer system, or computer network, he shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

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.

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.

Sec. 67 Transfer of the case to another court cannot be allowed on the ground the sec 6. Another evidence **involving pornographic act of the case will embrass the lady presiding judge. [Fatima Rishwana v. State Rap. by ACP, Chennai, 2005 (1) Crimes 121 (SC)].**

68. Power of Controller to give directions—(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

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 State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

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, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Comments

Any computer, computer system or computer network can be declared protected system by the Government by notification. Only authorised person can have access to the protected system. Any person who secures access or attempts to secure access to a protected system in contravention of the provision shall be punished with imprisonment up to ten years and shall also be liable to fines.

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

Comments

For obtaining any licence or Digital Signature Certificate if any person makes any misrepresentation or suppresses any material fact, he shall be punished with imprisonment up to two years, or with fine up to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy—Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine extend may extend to one lakh rupees, or with both.

Comments

Any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses the same to any other person then he shall be punished with imprisonment up to two years, or with fine up to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars—(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that :

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension revocation.

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

Comments

If any person publishes a Digital Signature Certificate or otherwise makes it available to any other person with the knowledge that (i) the Certifying Authority listed in the certificate has not issued it; or (ii) the subscriber listed in the certificate has not accepted it; or (iii) the certificate has been revoked or suspended unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation, he shall be punished with imprisonment up to two years or with fine up to one lakh rupees, or with both.

74. Publication for fraudulent purpose—Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Comments

Any person who knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose, he shall be punished with imprisonment up to two years, or with fine up to one lakh rupees, or with both.

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

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation—Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation :

Provided that where it is established to the satisfaction of the court adjudicating the cofiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments—No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences—Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Chapter XII

Network Service Providers Not to be Liable in Certain Cases

79. Network service providers not to be liable in certain cases—For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation—For the purposes 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.

Chapter XIII

Miscellaneous

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 authorised 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 sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or sent 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.

81. Act to have overriding effect—The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

[1][**81A. Application of the Act to electronic cheque and truncated cheque**—(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881), by the Central Government in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under sub-section (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or both Houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulument shall be without prejudice to the validity of anything previously done under that notification.

Explanation—For the purposes of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instrument Act, 1881 (26 of 1881).]

82. Controller, Deputy Controller and Assistant Controller to be public servants—The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

---

1. Ins. by Act 55 of 2002, sec. 13 (w.e.f. 6-2-2003).

83. Power to give directions—The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith—No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him,the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done n pursuance of this Act or any rule, regulation or order made thereunder.

85. Offences by companies—(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributed to any neglect on the part of, any director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation—For the purposes of this section,—

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

86. Removal of difficulties—(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government

may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules—(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely :

(a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 6;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;

(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;

(g) other standards to be observed by the Controller under clause (b) of sub-section (2) of section 20;

(h) the requirements which an applicant must fulfil under sub-section (2) of section 21;

(i) the period of validity of licence granted under clause (a) of sub-section (3) of section 22;

(j) the form in which an application for licence may be made under sub-section (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for licence under clause (d) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a licence and the fee payable thereof under section 23;

(n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(p) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

(r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;

(t) the salary and a allowances and other conditions of service of other officers and employees under sub-section (3) of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub-section (3) of section 57;

(v) any other power of a civil court required to be prescribed under clause (g) of sub-section (2) of section 58; and

(w) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each

House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both House agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee—(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulation Advisory Committee shall advise—

(a) the Central Government either generally as regards any rules or for any other purposes connected with this Act;

(b) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

Comments

The Central Government has constituted the "Cyber Regulation Advisory Committee" consisting of the following, namely—

1.	Minister, Information Technology	Chairman
2.	Secretary, Legislative Department	Member
3.	Secretary, Ministry of Information Technology	Member
4.	Secretary, Department of Telecommunication	Member
5.	Finance Secretary	Member
6.	Secretary, Ministry of Defence	Member

7.	Secretary, Ministry of Home Affairs	Member
8.	Secretary, Ministry of Commerce	Member
9.	Deputy Governor, Reserve Bank of India	Member
10.	Shri T.K. Vishwanathan, Presently Member Secretary, Law Commission	Member
11.	President, NASSCOM	Member
12.	President, Internet Service Providers Association	Member
13.	Director, Central Bureau of Investigation	Member
14.	Controller of Certifying Authority	Member
15.	Information Technology Secretary by rotation from the States	Member
16.	Director-General of Police by rotation from the states	Member
17.	Director, IIT by rotation from the IITs	Member
18.	Representative of CII	Member
19.	Representative of FICCI	Member
20.	Representative of ASSOCHAM	Member
21.	Senior Director, Ministry of Information Technology	Secretary

N.B.—The Committee may co-opt any person as Member based on specific meeting, *Vide* G.S.R. 790 (E), dated 17th October, 2000.

89. Power of Controller to make regulations—(1) The Controller may, after consultation with the Cyber Regulation Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely :

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause [1][(n)] of section 18;

1. Subs. vide S.O. 1015 (E), dated 19th September, 2002, for "(m)" (w.e.f. 19-9-2002).

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19.

(c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying Authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35;

(g) the manner by which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (2) of section 42.

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

90. Power of State Government to make rules—(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely—

(a) the electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6;

(c) any other matter which is required to be provided by rules by the State Government.

91. Amendment of Act 45 of 1860—The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

92. Amendment of Act 1 of 1872—The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

93. Amendment of Act 18 of 1891—The Bankers Book Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1934—The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

The First Schedule

(See section 91)

Amendments to the Indian Penal Code

(45 of 1860)

1. After section 29, the following section shall be inserted, namely :

"*29A. Electronic record*—The words "electronic record" shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000."

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "whoever makes any false documents or part of a document with intent to cause damage or injury", the words "whoever makes any false documents or false electronic record or part of a document or electronic record with intent to cause damage or injury" shall be substituted.

9. In section 464,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely—

A person is said to make a false document or false electronic record—

First—Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority

of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration."

(b) after *Explanation 2,* the following *Explanation* shall be inserted at the end, namely :

'Explanation 3—For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000'.

10. In section 466—

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;

(b) the following *Explanation* shall be inserted at the end, namely :

"Explanation—For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of sub-section 2 of the Information Technology Act, 2000.

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the

document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 474, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely :

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code."

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

The Second Schedule

(See section 92)

Amendments to the Indian Evidence Act, 1872

(1 of 1872)

1. In section 3,—

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "Indian", the following shall be inserted, namely :

'the expressions "Certifying Authority", "digital

signature", "Digital Signature Certificate", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'

2. In section 17, for the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. After section 22, the following section shall be inserted, namely :

"22A. *When oral admission as to contents of electronic records are relevant*—Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely—

"39. *What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers*—When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After section 47, the following section shall be inserted, namely—

"*47A. Opinion as to digital signature when relevant*—When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely—

'*65A. Special provisions as to evidence relating to electronic record*—The contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. Admissibility of electronic records—(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely—

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the

computer was operating properly or, if not; then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say—

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device

or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section—

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process'.

10. After section 67, the following section shall be inserted, namely—

"*67A. Proof as to digital signature*—Except in the case of a secure digital signature if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved."

11. After section 73, the following section shall be inserted, namely—

"*73A. Proof as to verification of digital signature*—In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000."

12. After section 81, the following section shall be inserted, namely—

"81A. Presumption as to Gazettes in electronic forms—The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. After section 85, the following sections shall be inserted, namely—

"85A. Presumption as to electronic agreements—The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

85B. Presumption as to electronic records and digital signatures—(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature."

85C. Presumption as to Digital Signature Certificates—The Court

shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

14. After section 88, the following section shall be inserted, namely :

"88A. Presumption as to electronic messages—The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000."

15. After section 90, the following section shall be inserted, namely :

"90A. Presumption as to electronic records five years old—Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This *Explanation* applies also to section 81A."

16. For section 131, the following section shall be substituted, namely—

"131. Production of documents or electronic records which another person, having possession, could refuse to produce—No one shall be

compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production."

The Third Schedule

(See section 93)

Amendments to the Bankers' Book Evidence Act, 1891

(18 of 1891)

1. In section 2,—

(a) for clause (3), the following clause shall be substituted, namely—

'(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;'

(b) for clause (8), the following clause shall be substituted, namely—

'(8) "certified copy" means when the books of a bank,—

(a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'

2. After section 2, the following section shall be inserted, namely—

"*2A. Conditions in the printout*—A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely—

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his

knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

The Fourth Schedule

(See section 94)

Amendment to the Reserve Bank of India Act, 1934

(2 of 1934)

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely :

"(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-I, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers."

Appendix 2

The Information Technology (Certifying Authorities) Rules, 2000[1]

In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the application and other guidelines for Certifying Authorities, namely—

1. Short title and commencement—(1) These Rules may be called the Information Technology (Certifying Authorities) Rules, 2000.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these Rules, unless the context otherwise requires—

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

(b) "applicant" means Certifying Authority applicant;

(c) "auditor" means any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognised by the Controller for conducting technical audit of operation of Certifying Authority;

(d) "Controller" means Controller of Certifying Authorities appointed under sub-section (1) of section 17 of the Act;

1. *Vide* G.S.R. 789 (E), dated 17th October, 2000, published in the Gazette of India, Extra, Pt. II, Sec. 3(i), dated 17th October, 2002.

(e) "Digital Signature Certificate" means Digital Signature Certificate issued under sub-section (4) of section 35 of the Act;

(f) "information asset" means all information resources utilised in the course of any organisaton's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks);

(g) "licence" means a licence granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;

(h) "licensed Certifying Authority" means Certifying Authorities for the issue of Digital Signature Certificates under these rules;

(i) "person" shall include an individual; or a company or association or body of individuals; whether incorporated or not; or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments;

(j) "Schedule" means a schedule annexed to these rules;

(k) "subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

(l) "trusted person" means any person who has—

(i) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority; or

(ii) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities;

(m) words and expressions used herein and not defined but defined in Schedule-IV shall have the meaning respectively assigned to them in that schedule.

3. The manner in which information be authenticated by means of Digital Signature—A Digital Signature shall,—

(a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again;

(b) use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematically related "keys"—one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form,

the process termed as hash function shall be used in both creating and verifying a Digital Signature.

Explanation—Computer equipment and software utilising two such keys are often termed as "asymmetric cryptography".

4. Creation of Digital Signature—To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; and the Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record.

5. Verification of Digital Signature—The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifer shall check—

(i) if the Digital Signature was created using the corresponding private key; and

(ii) if the newly computed hash result matches the original result which was transformed into Digital Signature during the signing process. The verification software will confirm the Digital Signature as verified if—

(a) the signer's private key was used to digitally sign

the electronic record, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and

(b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

6. Standards—The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority's functions are as under :

The Product	The Standard
Public Key Infrastructure	PKIX
Digital Signature Certificate and Digital Signatures revocation list	X. 509. Version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X. 500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key Algorithm	DSA and RSA
Digital Hash Function	MD5 and SHA-1
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request

	PKCS#12 Portable format for storing/transporting a user's private keys and certificates.
Distinguished Name	X.520
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10

7. Digital Signature Certificate Standard—All Digital Signature Certificates issued by the Certifying Authorities shall conform to *ITU X. 509 version 3 standard* as per rule 6 and shall *inter alia* contain the following data, namely—

(a) Serial Number (assigning of serial number to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate);

(b) Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate);

(c) Issuer Name (name of the Certifying Authority who issued the Digital Signature Certificate);

(d) Validity period of the Digital Signature Certificate;

(e) Name of the subscriber (whose public key the Certificate identifies); and

(f) Public Key information of the subscriber.

8. Licensing of Certifying Authorities—(1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely—

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or professions;

(b) a company having—

(i) paid-up capital of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees :

Provided that no company in which the equity share capital held in aggregated by the Non-resident Indians, Foreign

Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence :

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being the Hindu Undivided Family, firm or company :

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company.

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company—

(i) unless such a company acquired or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(c) a firm having—

(i) capital subscribed by all partners of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees :

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners;

Provided also that the partners referred to in the second provision shall not include Non-resident Indian and foreign national:

Provided also that the partnership of a firm referred to in the second proviso whose net worth has ben determined on the basis of such partners, shall not sell or transfer its capital held in such firm—

(i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Contoller.

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation—For the purpose of this rule—

(i) "company" shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act, 1961 (43 of 1961);

(ii) "firm", "partner" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;

(iii) "foreign" company" shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act, 1961 (43 of 1961);

(iv) "net worth" shall have the meaning assigned to it in clause (ga) of sub-section (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

(v) "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act, 1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall[1] [furnish a performance bond in the form of a banker's guarantee] from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than [fifty lakhs] of rupees and the [performance bond in the form of banker's

1. Subs. *vide* G.S.R. 902 (E), dated 21st November, 2003 (w.e.f. 27-11-2003).

guarantee] shall remain valid for a period of six years from the date of its submission :

Provided that the company and firm referred to in the second provio to clause (b) and the second proviso to clause (c) of sub-rule (1) shall [furnish a performance bond in the form of a banker's guarantee] for [one crore] of rupees :

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the [performance bond in the form of banker's guarantee] may be invoked—

(a) when the Controller has suspended the licence under sub-section (2) of section 25 of the Act; or

(b) for payment of an offer of compensation made by the Controller; or

(c) for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or

(d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's licence or operation is discontinued; or

(e) any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation—"transfer of operation" shall have the meaning assigned to it in clause (47) of section 2 of the Income-tax Act, 1961 (43 of 1961).

9. Location of the Facilities—The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.

10. Submission of Application—Every application for a licensed Certifying Authority shall be made to the Controller—

(i) in the form given at Schedule I; and

(ii) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall *inter alia* include—

(a) a Certification Practice Statement (CPS);

(b) a statement including the procedures with respect to identification of the applicant;

(c) a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;

(d) certified copies of the business registration documents of Certifying Authority that intends to be licensed;

(e) a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;

(f) an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Authority;

(g) an undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;

(h) an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2)of rule 8 within one month of Controller indicating his approval for the grant of licence to operate as a Certifying Authority;

(i) any other information required by a Controller.

11. Fee—(1) The application for the grant of a licence shall be accompanied by a non-refundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority's licence shall be accompanied by a non-

refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

12. Cross Certification—(1) The licensed Certifying Authority shall have arrangement for cross certification with other licensed Certifying Authorities within India which shall be submitted to the Controller before the commencement of their operations as per rule 20 :

Provided that any dispute arising as a result of any such arrangement between the Certifying Authorities; or between Certifying Authorities or Certifying Authority and the Subscriber, shall be referred to the Controller for arbitration or resolution.

(2) The arrangement for Cross Certification by the licensed Certifying Authority with a Foreign Certifying Authority along with the application, shall be submitted to the Controller in such form and in such manner as may be provided in the regulations made by the Controller and the licensed Certifying Authority shall not commence cross certification operations unless it has obtained the written or digital signature approval from the Controller.

13. Validity of licence—(1) A licence shall be valid for a period of five years from the date of its issue.

(2) The licence shall not be transferable.

14. Suspension of Licence—(1) The Controller may by order suspend the licence in accordance with the provisions contained in sub-section (2) of section 25 of the Act.

(2) The licence granted to the persons referred to in clause (a) to (c) of sub-rule (1) of rule 8 shall stand suspended when the [1][performance bond in the form of banker's guarantee furnished] by such persons is invoked under sub-rule (2) of that rule.

15. Renewal of licence—(1) The provisions of rule 8 to rule 13, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed Certifying Authority.

---

1. Subs. *vide* G.S.R. 902 (E), dated 21st November, 2003, (w.e.f. 27-11-2003).

(2) A Certifying Authority shall submit an application for the renewal of its licence not less than forty-five days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

16. Issuance of Licence—(1) Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he may deem fit, grant or renew the licence or reject the application :

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed Certifying Authority is approved, the applicant shall—

(a) submit a performance bond or furnish a banker's guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 9; and

(b) execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the rules made thereunder.

17. Refusal of Licence—The Controller may refuse to grant or renew a licence if—

(i) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

(ii) the applicant is in the course of being wound up or liquidated; or

(iii) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

(iv) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the

conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or

(v) the Controller has invoked performance bond or banker's guarantee; or

(vi) a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

(vii) a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

(viii) the audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or

(ix) a Certifying Authority fails to comply with the directions of the Controller.

18. Governing Laws—The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

19. Security Guidelines for Certifying Authorities—(1) The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule II and Schedule III respectively.

(i) The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation;

(ii) Provided that any change made by the Certifying Authority in the Information Technology and Security

Policy shall be submitted by it within two weeks to the Controller.

20. Commencement of Operation by Licensed Certifying Authorities—The licensed Certifying Authority shall commence its commercial operation of generation and issue of Digital Signature only after—

(a) it has confirmed to the Controller the adoption of Certification Practice Statement;

(b) it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller;

(c) the installed facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 31; and

(d) it has submitted the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

21. Requirement Prior to Cessation as Certifying Authority—Before ceasing to act as a Certifying Authority, a Certifying Authority shall,—

(a) give notice to the Controller of its intention to cease acting as a Certifying Authority :

Provided that the notice shall be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence;

(b) advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;

(c) notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unprovoked or unexpired Digital Signature Certificate issued by it :

Provided that the notice shall be given sixty days before ceasing to act as a Certifying Authority or sixty days

before the date of expiry of unrevoked or unexpired Digital Signature Certificate, as the case may be;

(d) the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;

(e) revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;

(f) make a reasonable effort to ensure that discontinuing its certification services cause minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates;

(g) make reasonable arrangements for preserving the records for a period of seven years;

(h) pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry;

(i) after the date of expiry mentioned in the licence, the Certifying Authority shall destroy the certificate-signing private key and confirm the date and time of destruction of the private key to the Controller.

22. Database of Certifying Authorities—The Controller shall maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing *inter alia* the following details :

(a) the name of the person/names of the Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorised representatives;

(b) the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognised foreign Certifying Authority to digitally sign Digital Signature Certificate;

(c) current and past versions of Certification Practice Statement of Certifying Authority;

(d) time stamps indicating the date and time of—

(i) grant of licence;

(ii) confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority;

(iii) commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority;

(iv) revocation or suspension of licence of Certifying Authority;

(v) commencement of operation of Cross Certifying Authority;

(vi) issue of recognition of foreign Certifying Authority;

(vii) revocation or suspension of recognition of foreign Certifying Authority.

23. Digital Signature Certificate—The Certifying Authority shall for issuing the Digital Signature Certificates, while complying with the provisions of section 35 of the Act, also comply with the following, namely :

(a) the Digital Signature Certificate shall be issued only after a Digital Signature Certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it :

Provided that the application form contains, *inter alia*, the particulars given in the modal Form given in Schedule IV;

(b) no interim Digital Signature Certificate shall be issued;

(c) the Digital Signature Certificate shall be generated by the Certifying Authority upon receipt of an authorised and validated request for :

(i) new Digital Signature Certificates;

(ii) Digital Signature Certificates renewal.

(d) the Digital Signature Certificate must contain or incorporate, by reference such information, as is sufficient to locate or identify one or more repositories in which revocation or suspension of the Digital

Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked;

(e) the subscriber identity verification method employed for issuance of Digital Signature Certificate shall be specified in the Certification Practice Statement and shall be subject to the approval of the Controller during the application for a licence;

(f) where the Digital Signature Certificate is issued to a person (referred to in this clause as a New Digital Signature Certificate) on the basis of another valid Digital Signature Certificate held by the said person (referred in this clause as an Originating Digital Signature Certificate) and subsequently the originating Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new Digital Signature Certificate;

(g) the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted;

(h) if the subscriber accepts the issued Digital Signature Certificate, the Certifying Authority shall publish a signed copy of the Digital Signature Certificate is a repository;

(i) where the Digital Signature Certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact, or otherwise, that affects the validity or reliability of such Digital Signature Certificate, it shall notify the same to the subscriber immediately;

(j) all Digital Signature Certificates shall be issued with a designated expiry date.

24. Generation of Digital Signature Certificate—The generation of the Digital Signature Certificate shall involve :

(a) receipt of an approved and verified Digital Signature Certificate request;

(b) creating a new Digital Signature Certificate;

(c) binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner;

(d) issuing the Digital Signature Certificate and the associated public key for operational use;

(e) a distinguished name associated with the Digital Signature Certificate owner; and

(f) a recognised and relevant policy as defined in Certification Practice Statement.

25. Issue of Digital Signature Certificate—Before the issue of the Digital Signature Certificate, the Certifying Authority shall—

(i) confirm that the user's name does not appear in its list of compromised users;

(ii) comply with the procedures as defined in his Certification Practice Statement including verification of identification and/or employment;

(iii) comply with all privacy requirements;

(iv) obtain a consent of the person requesting the Digital Signature Certificate, that the details of such Digital Signature Certificate can be published on a directory service.

26. Certificate Lifetime—(1) A Digital Signature Certificate,—

(a) shall be issued with a designated expiry date;

(b) which is suspended shall return to the operational use, if the suspension is withdrawn in accordance with the provisions of section 37 of the Act;

(c) shall expire automatically upon reaching the designated expiry date at which time the Digital Signature Certificate shall be archived;

(d) on expiry, shall not be re-used.

(2) The period for which a Digital Signature Certificate has been issued shall not be extended, but a new Digital Signature Certificate may be issued after the expiry of such period.

27. Archival of Digital Signature Certificate—A Certifying Authority shall archive—

(a) applications for issue of Digital Signature Certificates;

(b) registration and verification documents of generated Digital Signature Certificates;

(c) Digital Signature Certificates;
(d) notices of suspension;
(e) information of suspended Digital Signature Certificates;
(f) information of revoked Digital Signature Certificates;
(g) expired Digital Signature Certificates,

for a minimum period of seven years or for a period in accordance with legal requirement.

28. Compromise of Digital Signature Certificate—Digital Signature Certificates in operational use that become compromised shall be revoked in accordance with the procedure defined in the Certification Practice Statement of Certifying Authority.

Explanation—Digital Signature Certificates shall,—

(a) be deemed to be compromised where the integrity of—
  (i) the private key associated with the Digital Signature Certificate is in doubt;
  (ii) the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise for malicious or unlawful purposes;
(b) remain in the compromised state for only such time as it takes to arrange for revocation.

29. Revocation of Digital Signature Certificate—(1) Digital Signature Certificate shall be revoked and become invalid for any trusted use where—

(a) there is a compromise of the Digital Signature Certificate owner's private key;
(b) there is a misuse of the Digital Signature Certificate;
(c) there is a misrepresentation or errors in the Digital Signature Certificate;
(d) the Digital Signature Certificate is no longer required.

(2) The revoked Digital Signature Certificate shall be added to the Certificate Revocation List (CRL).

30. Fees for issue of Digital Signature Certificate—(1) The Certifying Authority shall charge such fee for the issue of Digital Signature Certificate as may be prescribed by the Central Government under sub-section (2) of section 25 of the Act.

(2) Fee may be payable in respect of access to Certifying Authority's X. 500 directory for certificate downloading. Where

fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.

(3) Fees may be payable in respect of access to Certifying Authority's X. 500 directory service for certificate revocation or status information. Where fees are payable, Certifying Authority shall provide an up to-date fee schedule to all its subscribers and users, this may be done by publishing the fee schedule to a nominated website.

(4) No fee is to be levied for access to Certification Practice Statement via Internet. A fee may be charged by the Certifying Authority for providing printed copies of its Certification Practice Statement.

31. Audit—(1) The Certifying Authority shall get is operations audited annually by an auditor and such audit shall include *inter alia* :

(i) security policy and planning;
(ii) physical security;
(iii) technology evaluation;
(iv) Certifying Authority's services administrations;
(v) relevant Certification Practice Statement;
(vi) compliance to relevant Certification Practice Statement;
(vii) contracts/agreements;
(viii) regulations prescribed by the Controller;
(ix) policy requirements of Certifying Authority Rules, 2000.

(2) The Certifying Authority shall conduct,—

(a) half years audit of the security policy, personal security and planning of its operation;
(b) a quarterly audit of its repository.

(3) The Certifying Authority shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities.

32. Auditor's relationship with Certifying Authority—(1) The auditor shall be independent of the Certifying Authority being audited and shall not be a software or hardware vendor

which is, or has been providing services or supplying equipment to the said Certifying Authority.

(2) The auditor and the Certifying Authority shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

33. Confidential Information—The following information shall be confidential, namely :

(a) Digital Signature Certificate application, whether approved or rejected;

(b) Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital Signature information;

(c) subscriber agreement.

34. Access to Confidential Information—(1) Access to confidential information by Certifying Authority's operational staff shall be on a "need-to-know" and "need-to-use" basis.

(2) Paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 shall be kept in secure and locked container or filing system, separately from all other records.

(3) The confidential information shall not be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

Schedule I

[*See* rule 10]

Form for Application for Grant of Licence to be a Certifying Authority

For Individual

1. Full Name * ..... Last Name/Surname.....First Name.....Middle Name .....

2. Have you ever been known by any other name ? If Yes, Last Name/Surname.....First Name.....Middle Name .....

3. Address,

A. Residential Address * Flat/Door/Block No. .....

Name of Premises/Building/Village..... Road/Street/Lane/ Post Office ..... Area/Locality/Taluka/Sub-Division.....Town/City/District .....

State/Union Territory.....Pin.....Telephone No. .....Fax.....Mobile Phone No. .....

B. Office Address * Name of Office ..... Flat/Door/ Block No. ..... Name of Premises/Building/Village .....Road/Street/Lane/Post Office..... Area/Locality/ Taluka/Sub-Division..... Town/City/District ..... State/Union Territory..... Pin .....Telephone No. ..... Fax .....

4. Address for Communication Tick [√] as applicable A [] B []

5. Father's Name * Last Name/Surname ..... First Name ..... Middle Name .....

6. Sex * (For Individual Applicant only) Tick [√] as applicable: Male/ Female

7. Date of Birth (dd/mm/yy) * .....

8. Nationality * .....

9. Credit Card Details/Credit Card Type ..... Credit Card No. ..... Issued By .....

10. E-mail Address .....

11. Web URL address .....

12. Passport Details #Passport No. ..... Passport issuing authority ..... Passport expiry date (dd/mm/ yy).....

13. Voter's Identity Card No. .....

14. Income Tax PAN No. .....

15. ISP Details ISP Name * ..... ISP's Website Address, if any .....Your User Name at ISP, if any .....

16. Personnal Web page URL address, if any .....

17. Capital in the business or profession * Rs. ..... (Attach documentary proof) For Company/Firm/Body of Individuals/Association of Persons/Local Authority.

18. Registration Number * .....

19. Date of Incorporation/Agreement/Partnership .....

20. Particulars of Business, if any * Head Office ..... Name of Office .....Flat/Door/Block No. ..... Name

of Premises/Building/Village ..... Road/Street/Lane/Post Office ..... Area/Locality/Taluka/Sub-Division..... Town/City/District ..... Pin ..... State/Union Territory ..... Telephone No. .....Fax ..... Web page URL address, if any ..... No. of Branches ..... Nature of Business .....

21. Income Tax PAN No. *.....

22. Turnover in the last financial year Rs.....

23. Net worth * Rs. .....

(Attach documentary proof)

24. Paid up Capital * Rs.....

(Attach documentary proof)

25. Insurance Details Insurance Policy No. * ..... Insurer Company .....

26. Names, Addresses, etc., of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given in the next page) * No. of Partners/Members/Directors .....

Details of Partners/Members/Directors

A. Full Name ..... Last Name/Surname ..... First Name ..... Middle Name .....

B. Address Flat/Door/Block No. ..... Name of Premises/Building/Village ..... Road/Street/Lanes/Post Office ..... Area/Locality/Taluka/Sub-Division..... Town/City/District ..... State/Union Territory ..... Pin ..... Telephone No. ..... Fax No. ..... Mobile Phone No.....

C. Nationality ..... In case of foreign national, Visa details .....

D. Passport Details/Passport No. ..... Passport issuing authority ..... Passport expiry date .....

E. Voter's Identity Card No.....

F. Income Tax PAN No. .....

G. E-mail Address .....

H. Personal Web page URL, if any .....

27. Authorised Representative* Name ..... Flat/Door/Block No. ..... Name of Premises/Building/Village

..... Road/Street/Lane/Post Office ..... Area/ Locality/Taluka/Sub-Division ..... Town/City/District ..... Pin ..... State/Union Territory ..... Telephone No. ..... Fax ..... Nature of Business .....

28. Particulars of Organisation : * Name of Organisation ..... Administrative Ministry/Department ..... Under State/Central Government ..... Flat/Door/Block No. ..... Name of Premises/Building/Village ..... Road/ Street/Lane/Post Office ..... Area/Locality/Taluka/Sub Division ..... Town/City/District ..... Pin ..... State/Union Territory ..... Telephone No. ..... Fax ..... Web page URL Address ..... Name of the Head of Organisation ..... Designation ..... E-mail Address .....

29. Bank Details Bank Name ..... Branch* ..... Bank Account No. * ..... Type of Bank Account .....

30. Whether bank draft/pay order for licence fee enclosed*: Y/N

If yes, Name of Bank ..... Draft/pay order No. ..... Date of Issue ..... Amount .....

31. Location of facility in India for generation of Digital Signature Certificate* .....

32. Public Key@ .....

33. Whether undertaking for [Performance Bond in the form of banker's guarantee] attached* : Y/N

(Not applicable if the applicant is a Government Ministry/ Department/Agency/Authority)

34. Whether Certification Practice Statement is enclosed* : Y/N

35. Whether certified copies of business registration document are enclosed : Y/N

(For Company/ Firm/ Body of Individuals/Association of Persons/ Local Authority)

If yes, the documents attached :

(i) .....

(ii) .....

(iii) .....

36. Any other information .....

Date

Signature of the Applicant

.....

Instructions : 1. Columns marked with * are mandatory.

2. For the columns marked with #, details for at least one is mandatory.

3. Column Nos. 1 to 17 are to be filed up by individual applicant.

4. Column Nos. 18 to 27 are to be filled up if applicant is a Company/Firm/Body of Individuals/Association of Persons/ Local Authority.

5. Column No. 28 is to be filled up if applicant is a Government organisation.

6. Column Nos. 29, 30, 31 and 34 are to be filled up by all applicants.

7. Column No. 32 is applicable only for application for renewal of licence.

8. Column No. 33 is not applicable if the applicant is a Government organisation.

Schedule II

[*See* rule 19 (2)]

Information Technology (IT) Security Guidelines

1. Introduction—This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organisations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organisations to develop internal processes that meet the guidelines set forth in this document.

The following words used in the Information Technology Security Guidelines shall be interpreted as follows :

* shall : The guideline defined is a mandatory requirement, and therefore must be complied with.
* should : The guidelines defined is a recommended

requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.

* must : The guideline defined is a mandatory requirement, and therefore must be complied with.
* may : The guidelines defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme—Successful implementation of a meaningful Information Security Programme rests with the support of top management. Until and unless the senior managers of the organisation understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows :

(a) Adoption of a security policy;
(b) Security risk analysis;
(c) Development and implementation of a information classification system;
(d) Development and implementation of the security standards manual;
(e) Implementation of the management security self-assessment process;
(f) On-going security programme maintenance and enforcement; and
(g) Training.

The principal task of the security implementation is to define the responsibilities of person within the organisation. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established.

When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its

access. It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. **Information Classification**—Information assets must be classified according to their sensitivity and their importance to the organisation. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organisation, it is necessary to advise them on which types of information are considered more sensitive, and how the organisation would like the sensitive information handled and protected. Classification, declassification, labelling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organisation will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorised disclosure/use could cause serious damage to the organisation, e.g., strategic planning documents.

Restricted is that classification of information of which unauthorised disclosure/use would not be in the best interest of the organisation and/or its customers, e.g., design details, computer software (programs, utilities), documentation, organisation personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g., published annual reports, periodicals.

While the above classifications are appropriate for a general organisation viewpoint, the following classification may be considered :

Top Secret : It shall be applied to information unauthorised disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret : This shall be applied to information unauthorised disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality : This shall be applied to information unauthorised disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher that confidential.

Restricted : This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purposes.

Unclassified : This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1. Site Design—(1) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.

(2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.

(3) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.

(4) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.

(5) External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground

level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.

(6) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

(7) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government shall be installed at the operational site.

(8) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.

(9) Any facility that supports mission-critical and sensitive applications must be located and designed for reparability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

4.2. Fire Protection—(1) Combustible materials shall not be stored within hundred meters of the operational site.

(2) Automatic fire detection, fire suppression system and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.

(3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.

(4) Periodic testing, inspection and maintenance of the fire equipment and fire suppression system shall be carried out.

(5) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

(6) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3. Environmental Protection—(1) Water detectors shall be installed under the raised floors thoroughout the operational site and shall be connected to audible alarms.

(2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

(3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.

(4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4. Physical Access—(1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.

(2) Biometric physical access security systems shall be installed to control and audit access to the operational site.

(3) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorised for limited physical access shall not be allowed to gain unauthorised access to restricted area within operational site.

(4) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.

(5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.

(6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

(7) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

(8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1. System Administration—(1) Each organisation shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.

(2) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

(3) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

(4) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organisation. Every instance of usage of administrator's passwords must be documented.

(5) Periodic review of the access rights of all users must be performed.

(6) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorised in writing by the System Administrator (Digitally signed e-mail may be acceptable).

(7) The System Administrator must take steps to safeguard classified information as prescribed by its owner.

(8) The System Administrator must authorise privileged access to users only on a need-to-know and need-to-do basis and also only after the authorisation is documented.

(9) Criteria for the review of audit trials/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

(10) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

(11) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.

(12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.

(13) The System Administrator should ensure that no generic user is enabled or active on the system.

5.2. Sensitive Information Control—(1) Information assets shall be classified and protected according to their sensitivity and criticality to the organisation.

(2) Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.

(3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

(4) All sensitive material shall be stamped or labelled accordingly.

(5) Storage media (i.e., floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.

(6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.

(7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g., hard disk/optical disk) and external (e.g., diskette, disk drive, tapes, *etc.*) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3. Sensitive Information Security—(1) Highly sensitive information assets shall be stored on secure removable media and

should be in an encrypted format to avoid compromise by unauthorised persons.

(2) Highly sensitive information shall be classified in accordance with para 3.

(3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorisation to segregated directories/files.

(4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

(5) Removable electronic storage media containing sensitive information and data must be clearly labelled and secured.

(6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4. Third Party Access—(1) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as these Information Technology security guidelines.

(2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g., outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.

(3) The external service/facility provider (e.g., outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5. Prevention of Computer Misuse—(1) Prevention, detection and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.

(2) Each organisation shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.

(3) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include :

(i) Prompt reporting of suspected breach;

(ii) Proper investigation and assessment of the nature of suspected breach;

(iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;

(iv) Remedial measures.

(4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.

(5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include :

(i) The role of the System Administrator, System Security Administrator and management;

(ii) Procedures for investigation;

(iii) Areas for security review; and

(iv) Subsequent follow-up action.

6. System Integrity and Security Measures

6.1. Use of Security Systems or Facilities—(1) Security controls shall be installed and maintained on each computer system and to prevent unauthorised access to data.

(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2. System Access Control—(1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.

(2) Access to information system resources like memory, storage devices, etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.

(3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game", etc., to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.

(4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorisations shall be developed, documented and implemented.

(5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.

(6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.

(7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.

(8) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

(9) Automatic time-out for terminal inactivity should be implemented.

(10) Audit trial of security-sensitive access and actions taken shall be logged.

(11) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.

(12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

(13) Activities of all remote users shall be logged and monitored closely.

(14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g., root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.

(15) The startup and shutdown procedure of the security must be automated.

(16) Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say, no user will be able to modify them except with the permission of System Administrator.

6.3. Password Management—(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords—

(i) Minimum of eight characters without leading or trailing blanks;

(ii) Shall be different from the existing password and two previous ones;

(iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

(iv) Shall not be shared, displayed or printed.

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess (e.g., user name, birth, date, month, standard words, etc.) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorised disclosure.

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4. Privileged User's Management—(1) System privileges shall be granted to users only on a need-to-use basis.

(2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.

(3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Authority.

(4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.

(5) Separate user IDs shall be allowed to the user performing privileged and normal (non-privileged) activities.

(6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5. User's Account Management—(1) Procedures for user account management shall be established to control to application systems and data. The procedures shall include the following :

(i) Users shall be authorised by the computer system owner to access the computer services.

(ii) A written statement of access rights shall be given to all users.

(iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

(iv) Where access to computer services is administered by service providers, ensure that the services providers do not provide access until the authorisation procedures have been completed. This includes the acknowledgement of receipt of the accounts by the users.

(v) A formal record of all registered users of the computer services shall be maintained.

(vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.

(vii) A periodic checks shall be carried out for redundant user accounts and access rights that are no longer required.

(viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions :

(i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator;

(ii) immediately upon the termination of the services of an individual;

(iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6. Data and Resource Protection—(1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

(2) The operating system or security system of the computer system shall :

(i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data object (e.g., file, programme) or groups of named objects, and the type of access allowed.

(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

(4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

(5) Application Programmer shall not be allowed to access the production system.

7. Sensitive Systems Protection—(1) Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies, etc., shall be used to complement the usage of passwords to access the computer system.

(2) For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.

(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1. Job Scheduling—(1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2. System Operations Procedures—(1) Procedure shall be established to ensure that only authorised and correct job stream and parameter changes are made.

(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.

(3) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.

(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/ reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management—(1) Responsibilities for media library management and protection shall be clearly defined and assigned.

(2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.

(3) Access to the media library (both on-site and off-site) shall be restricted to the authorised persons only. A list of personnel authorised to enter the library shall be maintained.

(4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.

(5) A media management system shall be in place to account for all media stored on-site and off-side.

(6) All incoming/outgoing media transfers shall be authorised by management and users.

(7) An independent physical inventory checks of all media shall be conducted at least every six months.

(8) All media shall have external volume identification Internal labels shall be fixed, where available.

(9) Procedures shall be in place to ensure that only authorised additional/removal of media from the library is allowed.

(10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4. Media Movement—(1) Proper records of all movements of computer tapes/disks between on-site and off-side media library must be maintained.

(2) There shall be procedures to ensure the authorised and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.

(3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention—(1) Back-up procedures shall be documented, scheduled and monitored.

(2) Up-to-date backups of all critical items shall be maintained to ensure the continued provisions of the minimum essential level of service. These items include :

(i) Data files

(ii) Utilities programmes

(iii) Databases
(iv) Operating system software
(v) Applications system software
(vi) Encryption keys
(vii) Pre-printed forms
(viii) Documentation (including a copy of the business continuity plans).

(3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.

(4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.

(5) Data backup is required for all systems including personal computers, servers and distributed systems and databases.

(6) Critical system data and file server software must have full backup taken weekly.

(7) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.

(8) Critical system data and file server software must have incremental backups taken daily.

(9) System that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.

(10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

(11) The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trails and Verification—(1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.

(2) Adequate audit trails shall be captured and certain

information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g., repeated unsuccessful logons, access attempts over a series of days) shall be analysed. This information includes such information as who, what, when, where and may special information such as :

(i) Success or failure of the event

(ii) Use of authentication keys, where applicable.

(3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as acesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include :

(i) Significant computer system events (e.g., configuration updates, system crashes);

(ii) Security profile changes;

(iii) Actions taken by computer operations system administrators, system programmers, and/or security administrators.

(4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases.

(5) The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further, there shall be a procedure that checks and corrects drift in the real time clock.

(6) Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.

(7) Computer records of application transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus—(1) Responsibilities and duties shall be assigned to ensure that all

file servers and personal computers are equipped with up-to-date virus protection and detection software.

(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies, etc., brought from outside shall be used on the data, file, PKI or computer server or personal computer on Internet and Internet without proper screening and verification by virus detection software.

(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of anti-virus software is loaded on all data, file, PKI servers and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organisation information assets. Such procedures *inter alia* shall include :

(i) Communication to other business partners and users who may be at risk from an infected resources;

(ii) Eradication and recovery procedures;

(iii) Incident report must be documented and communicated as per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software—Whenever computers or computer peripherals are relocated (e.g., for maintenance, installation at different sites or storage), the following guidelines shall apply—

(i) All removable media will be removed from the computer system and kept at secure location;

(ii) Internal drives will be overwritten, reformatted or removed as the situation may be;

(iii) If applicable, ribbons will be removed from printers;

(iv) All paper will be removed from printers.

13. Hardware and Software Maintenance—Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

(1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

(2) Maintenance of an inventory and configuration chart of hardware.

(3) Identification and use of security features implemented within hardware.

(4) Authorisation, documentation, and control of change made to the hardware.

(5) Identification of support facilities including power and air conditioning.

(6) Provision of an uninterruptible power supply.

(7) Maintenance of equipment and services.

(8) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.

(9) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

(10) Maintenance personnel will sign non-disclosure agreements.

(11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

(12) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorised personnel of the organisation.

(13) After maintenance, any exposed security parameters such as passwords, users IDs, and accounts will be changed or reset to eliminate any potential security exposures.

(14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software—(1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelnes prior to the signing of any contract, purchase or lease.

(2) Software which is capable of bypassing or modifying the security system or operating system, integrity features must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.

(3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.

(4) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.

(5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which th user has documented permission to install and test the software under evaluation.

(6) Illegally acquired or unauthorised software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorised software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software—(1) All system software options and parameters shall be reviewed and approved by the management.

(2) System software shall be comprehensively tested and its security functionality validated prior to implementation.

(3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

(4) Versions of system software installed on the computer system and communication devices shall be regularly updated.

(5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.

(6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

(7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".

(8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.

(9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.

(10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security—(1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.

(2) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.

(3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.

(4) Adequate backups of all documentation shall be

maintained and a copy of all critical documentation and manuals shall be stored off-site.

(5) Documentation shall be classified according to the sensitivity of its contents/implications.

(6) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security—(1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.

(2) The network configuration and inventories shall be documented and maintained.

(3) Prior authorisation of the Network Administrator shall be obtained for making any changes to the network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.

(4) Physical access to communications and network sites shall be controlled and restricted to authorised individuals only in accordance with para 4.4 pertaining to "Physical Access".

(5) Communication and network systems shall be controlled and restricted to authorised individuals only in accordance with para 6.2—System Access Control.

(6) As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.

(7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls—(1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network

with the external network. Firewall device should also be used to limit network connectivity for unauthorised use.

(2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organisation shall be physically and logically isolated from the Internet and any other external connection by a firewall.

(3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.

(4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity—(1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or network. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.

(2) All unused connection and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.

(3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.

(4) As far as possible, no Internet access should be allowed to database server-file server or server hosting sensitive data.

(5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator—(1) Each organisation shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

(2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide

physical, logical and procedural 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.

(3) System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorised access, virus infection and hacking.

(4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.

(5) Only authorised and legal software shall be used on the network.

(6) Shared computer systems, network devices used for business application shall comply with the requirement established in para 6—System Integrity and Security Measures.

21. Change Management

21.1. Change Control—(1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.

(2) A risk and impact analysis, classification and prioritisation process shall be established.

(3) No change to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.

(4) Owners/ Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.

(5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.

(6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.

(7) Version changes of application software and all system software installed on the computer systems and all communication

devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2. Testing of Changes to Production System—(1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.

(2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes : (i) Test objectives, (ii) A documented test plan, and (iii) Acceptance criteria.

21.3. Review of Changes—(1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

(2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.

(3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.

(4) Periodic management reports on the status of the changes implemented in the computer resource in the production system shall be submitted for management review.

22. Problem Management and Reporting—(1) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.

(2) A help desk shall be set up to assist users in the resolution of problems.

(3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness—(1) Emergency response procedures for all activities connected with computer operation

shall be developed and documented. These procedures should be reviewed periodically.

(2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Service—(1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.

(2) The business continuity plan shall be developed which *inter alia* include the procedures for emergency ordering of the equipment and availability of the services.

(3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response—(1) All security related incidents must be reported to a central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.

(2) All incidents reported, actions taken, follow-up actions, and other related informations shall be documented.

(3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which comprised the security of the system.

26. Disaster Recovery/Management—(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include :

(a) emergency procedures, describing the immediate actions to be taken in case of a major incident;

(b) fall-back procedures, describing the actions to be taken to relocate essential activities or support services to a backup site;

(c) restoration procedures, describing the action to be taken to return to normal operation at the original site.

(2) The documentation should include—

(a) definition of a disaster;

(b) condition for activating the plan;

(c) stages of a crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

Schedule III

[*See* rule 19(2)]

Security Guidelines for Certifying Authorities

1. Introduction—This document prescribes security guidelines for the management and operation of Certifying Autorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certifying Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as :

(1) Verification of registration, suspension and revocation request;

(2) Generation, issuance, suspension and revocation of Digital Signature Certificates, and

(3) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management—The Certifying Authority shall define Information Technology security policies for its operation on the lines defined in Schedule II and Schedule III. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel follow the policies.

3. Physical Controls, Site Location, Construction and Physical Access—(1) The site location, design, construction and physical security of the operational site of Certifying Authority shall be in accordance with para 4 of the Information Technology Security Guidelines given at Schedule II.

(2) Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorised individuals only in accordance with para 4 of the Information Technology Security Guidelines given at Schedule II.

(3) A Certifying Authority must—

(i) ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.2 of the Information Technology Security Guidelines given at Schedule II.

(ii) ensure that power and air-conditioning facilities are installed in accordance with para 4.1 of the Information Technology Security Guidelines given at Schedule II.

(iii) ensure that all removal media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.

(iv) ensure unescorted access to Certifying Authority's server is limited to those personnel identified on an access list.

(v) ensure that the exact location of Digital Signature Certification System shall not be publicly identified.

(vi) ensure that access security system is installed to control and audit access to the Digital Signature Certification System.

(vii) ensure that dual control over the inventory and access cards/keys are in place.

(viii) ensure that up-to-date list of personnel who possess the access cards/keys is maintained at the Certifying Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate to prevent unauthorised access.

(ix) ensure personnel not on the access list are properly escorted and supervised.

(x) ensure a site access log is maintained at the Certifying Authority's operational site and inspected periodically.

(4) Multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power. Electrical/ Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.

(5) Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinised and maintained for at least one year.

(6) A Certifying Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Guidelines given at Schedule II.

(7) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated

room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.

(8) Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system cabling, etc., shall be restricted to authorised personnel.

(9) Bye-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.

(10) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.

(11) Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.

(12) System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Guidelines given at Schedule II.

4. Media Storage—A Certifying Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with para 8.3 and para 8.4 of the Information Technology Security Guidelines given at Schedule II.

5. Waste Disposal—All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinsed before being destroyed or released for disposal.

6. Off-site Backup—A Certifying Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certifying Authority site.

7. Change and Configuration Management—(1) The components of the Certifying Authority infrastructure (e.g., cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical

security, system security, etc.) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.

(2) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.

(3) Software update and patches shall be reviewed for security implications before being implemented on Certifying Authority's system.

(4) Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented.

(5) Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented.

8. Network and Communication Security—(1) Certifying Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Guidelines given at Schedule II.

(2) Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.

(3) Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g., use of proxy servers) shall be implemented to protect the systems performing the functions of generation and management of Digital Signature Certificate from potential attacks.

(4) Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts

to compromise the confidentiality, integrity and availability of the certification function.

(5) Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed.

(6) Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

9. System Security Audit Procedures

9.1. Types of Event Recorded—(1) The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as :

(i) System start-up and shutdown;
(ii) Certifying Authority's application start-up and shutdown;
(iii) Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
(iv) Changes to keys of the Certifying Authority or any of his other details;
(v) Changes to Digital Signature Certificate creation policies, e.g., validity period;
(vi) Login and logoff attempts;
(vii) Unauthorised attempts at network access to the Certifying Authority's system;
(viii) Unauthorised attempts to access system files;
(ix) Generation of own keys;
(x) Creation and revocation of Digital Signature Certificates;
(xi) Attempts to initialise remove, enable, and disable subscribers and update and recover their keys;
(xii) Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

(2) Monitoring and Audit Logs

(i) A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained—

(a) Registration;
(b) Certification;
(c) Publication;
(d) Suspension; and
(e) Revocation.

(ii) Records and log files shall be reviewed regularly for the following activities—

(a) Misuse;
(b) Errors;
(c) Security violations;
(d) Executions of privileged functions;
(e) Change in access control lists;
(f) Change in system configuration.

(3) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/subordinate/entity which caused the event.

(4) A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as :

(i) Physical access logs;
(ii) System configuration changes and maintenance;
(iii) Personnel changes;
(iv) Discrepancy and compromise reports;
(v) Records of the destruction of media containing key material, activation data, or personal subscriber information.

(5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be consolidated, either electronically or manually, at a single location.

9.2. Frequency of Audit Log Monitoring—The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

9.3. Retention Period for Audit Log—The Certifying Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule II.

9.4. Protection of Audit Log—The electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion.

Manual audit information must be protected from unauthorised viewing, modification and destruction.

9.5. Audit Log Backup Procedures—Audit logs and audit summaries must be backed up or copied if in manual form.

9.6. Vulnerability Assessment—Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival—(1) Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven year after the date of its expiration. This requirement does not include the backup of private signature keys.

(2) Audit Information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.

(3) A second copy of all information retained or backed up must by stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection

from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours.

(4) All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properly constitutional warrant or such other legally enforceable document is produced.

(5) The Certifying Authority should verify the integrity of the backups at least once every six months.

(6) Information stored off-site must be periodically verified for data integrity.

11. Compromise and Disaster Recovery

11.1. Computing Resources, Software and/or Data are Corrupted—The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2. Secure Facility after a Natural or other Type of Disaster—The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3. Incident Management Plan—An incident management plan shall be developed and approved by the management. The plan shall include the following areas :

(i) Certifying Authority's certification key compromise;

(ii) Hacking of systems and network;

(iii) Breach of physical security;

(iv) Infrastructure availability;

(v) Fraudulent registration and generation of Digital Signature Certificates; and

(vi) Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas :

(i) Compromise control;

(ii) Notification to user community; (if applicable)

(iii) Revocation of affected Digital Signature Certificate (if applicable);

(iv) Responsibilities of personnel handling incidents;

(v) Investigation of service disruption;

(vi) Service restoration procedure;

(vii) Monitoring and audit trail analysis; and

(viii) Media and public relations.

12. Number of Persons Required Per Task—The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.

13. Identification and Authentication for Each Role—All Certifying Authority personnel must have their identity and authorisation verified before they are—

(i) included in the access list for the Certifying Authority's site.

(ii) included in the access list for physical access to the Certifying Authority's system;

(iii) given a certificate for the performance of their Certifying Authority role;

(iv) given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certifying Authority's signing certificates) must :

(i) be directly attributable to an individual;

(ii) not be shared;

(iii) be restricted to actions authorised for that role; and

(iv) procedural controls.

Certifying Authority's operations must be secured using techniques of authentication and encryption, when accessed across a shared network.

14. Personnel Security Controls—The Certifying Authority must ensure that all personnel performing duties with respect to its operation must :

(i) be appointed in writing;

(ii) be bound by contract or statute to the terms and conditions of the position they are to fill;

(iii) have received comprehensive training with respect to the duties they are to perform;

(iv) be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;

(v) not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; and

(vi) be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation.

15. Training Requirements—A Certifying Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in :

(i) relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certifying Authority;

(ii) all PKI software versions in use on the Certifying Authority's system;

(iii) all PKI duties they are expected to perform; and

(iv) disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirement—The requirements of para 15 must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel—A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

18. Key Management

18.1. Generation—(1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.

(2) The key generation process shall generate random key values that are resistant to known attacks.

18.2. Distribution of Keys—Keys shall be transferred from the key generation system to the storage device (if the key are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

18.3. Storage—(1) Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.

(2) The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and documented.

18.4 Usage—(1) A system and software integrity check shall be performed prior to Certifying Authority's key loading.

(2) Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control.

18.5. Certifying Authority's Public Key Delivery to Users—The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

19. Private Key Protection and Backup—(1) The Certifying Authority must protect its private keys from disclosure.

(2) The Certifying Authority must backup its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.

(3) The Certifying Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key—Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

21. Usage Periods for the Public and Private Keys

21.1. Key Change—(1) Certifying Authority and Subscriber keys shall be changed periodically.

(2) Key change shall be processed as per Key Generation guidelines.

(3) The Certifying Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.

(4) The Certifying Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks—such as signing a hash of the new key with the old key.

All keys must have validity periods of no more than five years.

Suggested validity period :

(a) Certifying Authority's root keys and associated certificates—five years;

(b) Certifying Authority's private signing key—two years;

(c) Subscriber Digital Signature Certificate key—three years;

(d) Subscriber Private Key—three years.

Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

21.2 Destruction—Upon termination of use of a Certifying Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

21.3. Key Compromise—(1) A procedure shall be pre-established to handle cases where a compromise of the Certifying Authority's Digital Signature private key has occurred. In such case, the Certifying Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.

(2) The Certifying Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.

(3) The Certifying Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.

(4) Archives of Certifying Authority's public keys shall be protected from unauthorised modification.

22. Confidentiality of Subscriber's Information—(1) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.

(2) Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy.

(3) A secure communication channel between Certifying Authority and its subscribes shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g., transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

Schedule IV

[See rule 23]

[1][Form A

Application form for Issue of Digital Certificate for Subscriber of Government and Banking Sector

Class of certificate applied	:	Certificate Required Individual/Server/ Web server
Certificate Validity	:	.....
Name	:	.....
E-mail Address	:	.....
Office Address	:	.....
(With Designation and	:	.....
Department) (Optional)	:	.....
	:	Telephone .....
Identification Details	:	Employee Identification No. ..... Passport No. ..... Any other ..... (Passport No./PAN Card No./ Voter's ID Card No./ Driving Licence No./PF No.)
In case the application is for a device, then details of Server/ Device for which the certificate is being applied for must be filled		Web Server ..... Services ..... IP address ..... URL/Domain Name ..... Physical Location .....

For Head of Office or JS (Admn.) for Government Sector/ Superior Authority for Banking Sector of Applicant

This is to certify that Mr./Ms.....has provided correct information in the "Application form for issue of Digital Certificate for subscriber of Government and Banking Sector" to the best of my knowledge and belief. I hereby authorise him/her, on behalf of my organisation to apply for obtaining Digital Certificate from CA for the purpose specified above.

Date .....

1. Amended by G.S.R. 285 (E), dated 23rd April, 2004.

Place.....

Name of Officer with Designation

(Signature of Officer with Stamp of Org./Office)

Office E-mail

Important Notice :

- This application form is to be filled by the applicant.
- All subscribers are advised to read Certificate Practice Statement of CA.
- All documents specified in CPS for each Certificate Class must be accompanied with this application form.
- Application form must be submitted in person.
- Incomplete/Inconsistent application is liable to be rejected.]

[1][Form B

Application Form for Issue of Digital Signature Certificate for Subscribers other than Government and Banking Sector

Class of certificate applied	:	Certificate Required Individual/Server/ Web server
Certificate Validity	:	.....
Name	:	.....
E-mail Address	:	.....
Officer Address	:	.....
(With Designation and	:	.....
Department) (Optional)	:	.....
	:	Telephone .....
Residential Address	:	.....
		.....
		.....
		Telephone .....
In case the application is for a		Web Server .....
device, then details of Server/		Services .....
Device for which the certificate is being applied for must be filled		IP address .....

1. Amended by G.S.R. 285 (E), dated 23rd April, 2004.

URL/Domain Name .....
Physical Location .....

Date .....

Place.....

(Signature of the Applicant)

Authentication of Identity and Proof of Residence

Copies of one or more of the following must be provided, as required by the Certifying Authority. Identity verification methods for the certificate applicant will be as per the procedure specified in the Certification Practice Statement (CPS) of the CA.

1. Passport
2. Election Card (Voter's ID)
3. Ration Card
4. Bank Accounts Details
5. Driving Licence
6. Any Other

Important Notice

- This application form is to be filled by the applicant.
- All subscribers are advised to read Certificate Practice Statement of CA.
- All documents specified in CPS for each Certificate Class must be accompanied with this application form.
- Application form must be submitted in person.
- Incomplete/Inconsistent application is liable to be rejected.]

Abbreviations

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
e-mail	Electronic Mail
FTP	File Transfer Protocol

ISDN	Integrated Service Digital Network
ITU	International Telecommunications Union
LAN	Local Area Network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
URL	Uniform Resource Locator
WAN	Wide Area Network

Appendix 3

The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000

In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely—

1. ***Short title and commencement***—(1) These rules may be called the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000.

(2) They shall come into force on the date of publication in the Official Gazette.

2. ***Definitions***—In these rules, unless the context otherwise requires—

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

(b) "agent" means a person duly authorised by a party to present an application or reply on its behalf before the Tribunal;

(c) "application" means an application made to the Tribunal under section 57;

(d) "legal practitioner" shall have the same meaning as is assigned to it in the Advocates Act, 1961 (25 of 1971);

(e) "Presiding Officer" means the Presiding Officer of the Tribunal;

(f) "Registrar" means the Registrar of the Tribunal and includes any officer to whom the powers and functions of the Registrar may be delegated;

(g) "registry" means the registry of the Tribunal;

(h) "section" means a section of the Act;

(i) "transferred application" means the suit or other proceeding which has been transferred to the tribunal under sub-section (1) of section 29;

(j) "Tribunal" means the Cyber Regulations Appellate Tribunal established under section 48.

3. *Procedure for filing applications*—(1) An application to the Tribunal shall be presented in Form 1 annexed to these rules by the applicant in person or by an agent or by a duly authorised legal practitioner, to the Registrar or sent by registered post addressed to the Registrar.

(2) The application under sub-rule (1) shall be presented in six complete sets in a paper-book form along with one empty file size envelop bearing full address of the respondent. Where the number of respondents is more one, sufficient number of extra paper-books together with required number of empty file size envelopes bearing the full address of each respondent shall be furnished by the applicant.

(3) The applicant may attach to and present with his application a receipt slips as in Form No. 1 which shall be signed by the Registrar or the officer receiving the applications on behalf of the Registrar in acknowledgement of the receipt of the application.

(4) Notwithstanding anything contained in sub rules (1), (2) and (3), the Tribunal may permit—

(a) more than one person to join together and file a single application if it is satisfied, having regard to the cause of action and the nature of relief prayed for, that they have the same interest in the service matter; or

(b) an Association representing the persons desirous of joining in a single application provided, however, that the application shall disclose the names of all the persons on whose behalf it has been filed.

4. Presentation and scrutiny of application—(1) The Registrar, or the officer authorised by the Registrar shall endorse on every application the date on which it is presented or deemed to have been presented under that rule and shall sign the endorsement.

(2) If, on scrutiny, the application is found to be in order, it shall be duly registered and given a serial number.

(3) If the application, on scrutiny, is found to be defective, and the defect noticed is formal in nature, the Registrar may allow the party to recitfy the same in his presence, and if the said defect is not formal in nature, the Registrar may allow the applicant such time to rectify the defect as he may deem fit.

(4) If the applicant fails to rectify the defect within the time allowed under sub-rule (3), the Registrar may, by order and for reasons to be recorded in writing, decline to register the application.

(5) An appeal against the order of the Registrar under sub-rule (4) shall be made within 15 days of the making of such order to the Tribunal whose decision thereon shall be final.

5. Place of filing application—The applicant shall file application with the Registrar.

6. Application fee—Every application filed with the Registrar shall be accompanied by a fee of Rs. 2,000/- (rupees two thousand) only which shall be either in the form of a crossed demand draft or a pay order drawn on a Scheduled bank in favour of the Registrar and payable at New Delhi.

7. Contents of application—(1) Every application filed under rule 3 shall set forth concisely under distinct heads, the grounds for such application and such grounds shall be numbered consecutively and typed in double space on one side of the paper.

(2) It shall not be necessary to present a seperate application to seek an interim order or direction if the application contains a prayer seeking an interim order or direction pending final disposal of the application.

(3) An application may, subsequent to the filing of application under section 57 of the Act, apply for an interim order or direction. Such an application shall, as far as possible, be in the same form as is prescribed for on application under section 57 and shall be accompanied by a fee of Rs. 5/- (Rupees five only) which shall be payable in court fee stamps affixed on such application.

8. Paper book, etc. to accompany the application—(1) Every application shall be accompanied by a paper book containing—

(i) a certified copy of the order against which the application has been filed;

(ii) copies of the documents relied upon by the applicant and referred to in the application; and

(iii) an index of documents.

(2) The documents referred to in sub-rule (1) may be attested by an advocate or by a gazetted officer.

(3) Where an application is filed by an agent, documents authorising him to act as such agent shall also be appended to the application.

Provided that where an application is filed by an advocate it shall be accompanied by a duly executed *'Vakalatnama'*.

9. Plural remedies—An application shall be based upon a single cause of action and may seek one or more reliefs provided they are consequential to one another.

10. Service of notice of application on the respondents—(1) A copy of the application in the paper-book shall ordinarily be served on each of the respondents by the Registrar in one of the following modes :

(i) hand delivery (dasti) through the applicant or through a process server; or

(ii) through registered post with acknowledgement due.

(2) Notwithstanding anything contained in sub-rule (1), the Registrar may, taking into account the number of respondents and their places of residence or work and other circumstances direct that notice of the application shall be served upon the respondents in any other manner including any manner of substituted service, as it appear to the Registrar just and convenient.

(3) Every applicant shall pay a fee for the service or execution of processes, in respect of an application where the number of respondents exceeds five, as under—

1. a sum of Rs. 50 (Rupees fifty) for each respondent in excess of five respondents; or

2. where the service is in such manner as the Registrar may direct under sub-rule (2), a sum not exceeding the actual charges incurred in effecting the service as may be determined by the Registrar.

(4) The fee for the service or execution of processes under sub-rule (3) shall be remitted by the applicant either in the form of a crossed Demand Draft drawn on a Scheduled Bank in favour of the Registrar and payable at the station where Registrar's office is situated or remitted through a crossed Indian Postal Order drawn in favour of the Registrar and payable in General Post Office of the station where the Tribunal is located.

(5) Notwithstanding anything contained in sub-rules (1), (2), (3) and (4), if the Tribunal is satisfied that it is not reasonably practicable to serve notice of application upon all the respondents, if may for reasons to be recorded in writing, direct that the application shall be heard notwithstanding that some of the respondents have not been served with notice of the application, provided that no application shall be heard unless—

- notice of the application has been served on the Government, if Government is respondent;
- notice of the application has been served on the authority which passed the order against which the application has been filed; and
- the Tribunal is satisfied that the interests of the respondents on whom notice of the application has not been served are adequately and sufficiently represented by the respondents on whom notice of the application has been served.

11. Filing of reply and other documents by the respondent—(1) The respondent shall file six complete sets containing the reply to the application along with the documents in a paper-book form with the Registrar within one month of the date of service of the notice of the application on him.

(2) The respondent shall also serve a copy of the reply along with copies of documents as mentioned in sub-rule (1) to the applicant or his advocate, if any, and file proof of such service with the Registrar. The Tribunal may, on application by the respondent, allow filing of the reply after the expiry of the period of one month.

12. Date and place of hearing to be notified—The Tribunal shall notify to the parties the date and the place of hearing of the application.

13. Sittings of the Tribunal—The Tribunal shall ordinarily hold its sittings at New Delhi :

Provided that, if at any time, the Presiding Officer of the Tribunal is satisfied that circumstances exist which render it necessary to have sittings of the Tribunal at any place other than New Delhi the Presiding Officer may direct to hold the sittings at any such appropriate place.

14. Decision on applications—(1) Tribunal shall draw up a calender for the hearing of transferred cases and as far as possible hear and decide the cases according to the calendar.

(2) Every application shall be heard and decided, as far as possible, within six months of the date of its presentation.

(3) For purposes of sub-rules (1) and (2), the Tribunal shall have the power to decline an adjournment and to limit the time for oral arguments.

15. Action on application for applicant's default—(1) Where on the date fixed for hearing of the application or on any other date to which such hearing may be adjourned, the applicant does not appear when the application is called on for hearing, the Tribunal may, in its discretion, either dismiss the application for default or hear and decide it on merit.

(2) Where an application has been dismissed for default and the applicant appears afterwards and satisfies the Tribunal that there was sufficient cause for his non-appearance when the application was called on for hearing, the Tribunal shall make an order setting aside the order dismissing the application and restore the same.

16. Hearing on application *ex-parte*—(1) Where on the date fixed for hearing the application or on any other date to which hearing is adjourned, the applicant appears and the respondents does not appear when the application is called on for hearing, the Tribunal may, in its discretion, adjourn or hear and decide the application *ex-parte*.

(2) Where an application has been heard *ex-parte* against a respondent or respondents, such respondents may apply to the Tribunal for an order to set it aside and if such respondent or respondents satisfy the Tribunal that the notice was not duly served, or that he or they were prevented by any sufficient cause

from appearing when the application was called on for hearing, the Tribunal may make an order setting aside the *ex-parte* hearing as against him or them upon such terms as it thinks fit, and shall appoint a day for proceeding with the application :

Provided that where the *ex-parte* hearing of the application is of such nature that it cannot be set aside as against one respondent only, it may be set aside as against all or any of the other respondents also :

Provided further that Tribunal shall not set aside *ex-parte* hearing of an application merely on the ground that there has been an irregularity in the service of notice, if it is satisfied that the respondent had notice of the date of hearing and had sufficient time to appear and answer the applicant's claim.

17. Adjournment of application—The Tribunal may on such terms as it deems fit and at any stage of the proceedings adjourn the hearing of the application.

18. Order to be signed and dated—Every order of the Tribunal shall be in writing and shall be signed and dated by the Presiding Officer.

19. Publication of orders—Such of the orders of the Tribunal as are deemed fit for publication in any report or the press may be released for such publication on such terms and conditions as the Tribunal may lay down.

20. Communication of orders to parties—Every order passed on an application shall be communicated to the applicant and to the respondent either in person or by registered post free of cost.

21. No fee for inspection of records—No fee shall be charged for inspecting the records of a pending application by a party thereto.

22. Orders and directions in certain cases—The Tribunal may make such orders or give such directions as may be necessary or expedient to give effect or in relation to its orders or to prevent abuse of its process or to secure the ends of justice.

23. Registration of legal practitioners clerks—(1) A clerk employed by a legal practitioner and permitted as such to have access to the records and to obtain copies of the order of the Tribunal in which the legal practitioner ordinarily practices shall be known as a "registered clerk".

(2) A legal practitioner desirous of registering his clerk shall make an application to the Registrar in Form 2.

(3) A legal practitioner shall have at a time not more than two registered clerks unless the Registrar by general or special order otherwise permits.

(4) A register of all the registered clerks shall be maintained in the office of the Registrar and after registration of the clerk, the Registrar shall direct the issue of an identity card to him which shall be non-transferable and shall be produced by the holder upon request by an officer or any other employee of the Tribunal.

(5) The identity card mentioned in sub-rule (4) shall be issued under the signatures of the Registrar of the Tribunal.

(6) Whenever a legal practitioner ceases to employ a registered clerk, he shall notify the fact at once to the Registrar by means of a letter enclosing therewith the identity card issued to his clerk and on receipt of such letter the name of the said registered clerk shall be struck off from the register.

24. Working hours of the Tribunal—Except on Saturday, Sunday and other holidays, the offices of the Tribunal shall, subject to any order made by the Presiding Officer, remain open daily from 10.00 a.m. to 5.00 p.m. but no work, unless it is of an urgent nature, shall be admitted after 4.30 p.m. on any working day.

25. Sitting hours of the Tribunal—The sitting hours of the Tribunal shall ordinarily be from 10.30 a.m. to 1.00 p.m. and 2.00 p.m. to 5.00 p.m. subject to any order made by the Chairman.

26. Powers and functions of the Registrar—(1) The Register shall have the custody of the records of the Tribunal and shall exercise such other functions as may be assigned to him under these rules or by the Presiding Officer.

(2) The Registrar may, with the approval of the Presiding Officer, delegate to another officer of the Tribunal any functions required by these rules to be exercised by the Registrar.

(3) In the absence of the Registrar, officer of the Tribunal authorised in writing by the Presiding Officer in his behalf may perform or exercise any of the functions and powers of the Registrar.

(4) The Registrar shall keep in his custody the official seal of the Tribunal.

(5) The Registrar shall, subject to any general or special direction by the Presiding Officer, affix the official seal of the Tribunal on any order, notice or other process.

(6) The Registrar shall have the power to authorise in writing the affixing of the seal of the Tribunal on a certified copy of any order of the Tribunal.

27. Additional powers and duties of Registrar—In addition to the powers conferred elsewhere in these rules, the Registrar shall have the following powers and duties subject to any general or special order of the Presiding Officer, namely :

(i) to receive all applications and other documents including transferred applications;

(ii) to decide all questions arising out of the scrutiny of the applications before they are registered;

(iii) to require any application presented to the Tribunal to be amended in accordance with the Act and the rules;

(iv) subject to the directions of the Tribunal, to fix dates of hearing of the applications or other proceedings and issue notices thereof;

(v) to direct any formal amendment of records;

(vi) to order grant of copies of documents to parties to the proceedings;

(vii) to dispose of all matters, relating to the service of notices of other processes, applications for the issue of fresh notices or for extending the time therefore;

(viii) to requisition records from the custody of any court or other authority;

(ix) to receive applications for the substitution of legal representatives of the decesased parties, during the pendency of the application;

(x) to receive and dispose of applications for substitution, except where the substitution would involve setting aside an order or abatement; and

(xi) to receive and dispose of application by parties for return of documents.

28. Seal and emblem—The official seal and emblem of the Tribunal shall be such as the Government may specify.

FORM 1

(*See* rule 4)

APPPLICATION UNDER SECTION 57 OF THE INFORMATION TECHNOLOGY ACT, 2000

For use in Tribunal's Office

Date of filing .....

OR

Date of receipt by post .....

Registration No. .....

Signature of Registrar

IN THE CYBER REGULATIONS APPELLATE TRIBUNAL

.....

.....

BETWEEN

A B ...APPLICANT

AND

C D .... RESPONDENT

Details of Application :

1. Particulars of the applicant—

(i) Name of the applicant

(ii) Name of Father/Husband

(iii) Designation and office in which employed

(iv) Office Address

(v) Address for service of all notice

2. Particulars of the respondent—

(i) Name and/or designation of the respondent

(ii) Office address of the respondent

(iii) Address for service of all notices

3. Particulars of the order against which application is made:

The application is against the following order :

(i) Order No.

(ii) Date

(iii) Passed by

(iv) Subject in brief

4. Jurisdiction of the Tribunal :

The applicant declares that the subject-matter of the order against which he wants redressal is within the jurisdiction of the Tribunal.

5. Limitation—

The applicant further declares that the application is within the limitation prescribed in section 57 of the Information Technology Act, 2000.

6. Fact of the case—

The facts of the case are given below—

(Give here a concise statement of facts in a chronological order, each paragraph containing as nearly as possible a separate issue, fact or otherwise)

7. Relief(s) sought—

In view of the facts mentioned in para 6 above, the applicant prays for the following relief(s)—

[Specify below the relief(s) sought explaining the ground for the relief(s) and the legal provisions (if any) relief upon].

8. Interim order, if prayed for :

Pending final decision on the application, the applicant seeks issue of the following interim order :

(Give here the nature of the interim order prayed for with reasons).

9. Details of the remedies exhausted—

The applicant declares that he has availed of all the remedies available to him under the relevant service rules, etc.

(Give here chronologically the details of representations made and the outcome of such representations).

10. Matter not pending with any other court, etc.—

The applicant further declares that the matter regarding which this application has been made is not pending before any court of law or any other authority or has been rejected by any court of law or other authority.

11. Details of Index—

An index in duplicate containing the details of the documents to be relied upon is enclosed.

12. List of enclosures—

Verification

I, ... (name of the applicant), S/o, D/o, W/o ..... age ..... working as ..... resident of ..... hereby verify that the contents from 1 to 13 are true to my personal knowledge and belief and that I have not suppressed any material facts.

Place :

Date :

Signature of applicant

To

The Registrar,
Cyber Regulation Appellate Tribunal
New Delhi

RECEIPT SLIP

Receipt of the application filed in the Cyber Regulation Appellate Tribunal by Shri/Smt. ..... working as ..... in the Office of ..... residing ..... acknowledged.

Form 2

(*See* rule 24)

APPLICATION FOR THE REGISTRATION OF A CLERK

1. Name of legal practitioner on whose behalf the clerk is to be registered.

2. Particulars of the clerk to be registered.

(i) Full name (in capitals)
(ii) Father's name
(iii) Age and date of birth
(iv) Place of birth
(v) Nationality
(vi) Educational qualifications

(vii) Particulars of previous employment, if any.

I, ... (clerk above named), do hereby affirm that the particulars relating to me are true.

3. Whether the legal practitioner has a clerk already registered in his employ and whether the clerk sought to be registered is in lieu of or in addition to the clerk already registered.

4. Whether the clerk sought to be registered is already registered as a clerk of any other legal practitioner and if so, the name of such practitioner.

I, ... (legal practitioner) certify that the particulars given above are true to the best of my information and belief and that I am not aware of any facts which would render undesirable the registration of the said..... (name) as a clerk.

Date :

Signature of legal practitioner

To

The Registrar of the Tribunal

.....

.....

.....

Notification Regarding Date of Enforcement of the Act

17th October, 2000

In exercise of the powers conferred by sub-section (3) of section 1 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby appoints 17th Day of October 2000 as the date on which the provisions of the said Act comes into force.

[No. 1 (20)/97-IID(NII)/F6(i)]

List of Chairman and Members of Cyber Regulation Advisory Committee

Notification

17th October, 2000

In exercise of the powers conferred by section 88 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby constitute the "Cyber Regulation Advisory Committee", consisting of the following, namely—

1.	Minister, Information Technology	Chairman
2.	Secretary, Legislative Department	Member
3.	Secretary, Ministry of Information Technology	Member
4.	Secretary, Department of Telecommunication	Member
5.	Finance Secretary	Member
6.	Secretary, Ministry of Defence	Member
7.	Secretary, Ministry of Home Affairs	Member
8.	Secretary, Ministry of Commerce	Member
9.	Deputy Governor, Reserve Bank of India	Member
10.	Shri T.K. Vishwanathan, Presently Member Secretary, Law Commission	Member
11.	President, NASSCOM	Member
12.	President, Internet Service Providers Association	Member
13.	Director, Central Bureau of Investigation	Member
14.	Controller of Certifying Authority	Member
15.	Information Technology Secretary by rotation from the States	Member
16.	Director General of Police by rotation from the states	Member
17.	Director, IIT by rotation from the IITs	Member
18.	Representative of CII	Member
19.	Representative of FICCI	Member
20.	Representative of ASSOCHAM	Member
21.	Senior Director, Ministry of Information Technology	Secretary

2. Travelling Allowance/Dearness Allowance, as per the Central Government rules, for the non-official members shall be borne the Ministry of Information Technology.

3. The Committee may co-opt any person as member based on specific meetings.

Appendix 4

The Information Technology (Certifying Authority) Regulations, 2001

In exercise of the powers conferred by clauses (c), (d), (e), and (g) of sub-section (2) of section 89 of the Information Technology Act, 2000 (21 of 2000), the Controller hereby, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, makes the following Regulations, namely :

1. Short title and commencement—(1) These Regulations may be called the Information Technology (Certifying Authority) Regulations, 2001.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these Regulations, unless the context otherwise requires,—

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

(b) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24 of the Act;

(c) "Certificate Revocation List" means a periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates;

(d) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17 of the Act;

(e) "Form" means the form appended to these Regulations;
(f) "Public Key Certificate" means a Digital Signature Certificate issued by Certifying Authority;
(g) "subscriber" means a person in whose name the Digital Signature Certificate is issued;
(h) Words and expressions used herein and not defined, but defined in the Act, shall have the meanings respectively assigned to them in the Act.

3. Terms and conditions of licence to issue Digital Signature Certificate—Every licence to issue Digital Signature Certificates shall be granted under the Act subject to the following terms and conditions, namely—

(i) General—

(a) The licence shall be valid for a period of five years from the date of issue.
(b) The licence shall not be transferable or heritable;
(c) The Controller can revoke or suspend the licence in accordance with the provisions of the Act.
(d) The Certifying Authority shall be bound to comply with all the parameters against which it was audited prior to issue of licence and shall consistently and continuously comply with those parameters during the period for which the licence shall remain valid.
(e) The Certifying Authority shall subject itself to periodic audits to ensure that all conditions of the licence are consistently complied with by it. As the cryptographic components of the Certifying Authority systems are highly sensitive and critical, the components must be subjected to periodic expert review to ensure their integrity and assurance.
(f) The Certifying Authority must maintain secure and reliable records and logs for activities that are core to its operations.
(g) Public Key Certificates and Certificate Revocation Lists must be archived for a minimum period of seven years to enable verification of past transactions.
(h) The Certifying Authority shall provide Time Stamping Service for its subscribers. Error of the Time Stamping clock shall not be more than 1 in 10^9.

(i) The Certifying Authority shall use methods, which are approved by the Controller, to verify the identity of a subscriber before issuing or renewing any Public Key Certificate.

(j) The Certifying Authority shall publish a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation.

(k) The Certifying Authority shall always assure the confidentiality of subscriber information.

(l) All changes in Certificate Policy and Certification Practice Statement shall be published on the website of the Certifying Authority and brought to the notice of the Controller well in advance of such publication. However, any change shall not contravene any provision of the Act, rule or regulation or made thereunder.

(m) The Certifying Authority shall comply with every order or direction issued by the Controller within the stipulated period.

(ii) Overall Management and Obligations—

(a) The Certifying Authority shall manage its functions in accordance with the levels of integrity and security approved by the Controller from time to time.

(b) The Certifying Authority shall disclose information on the assurance levels of the certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties.

(c) The Certifying Authority shall as approved, in respect of security and risk management controls continuously ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches.

(iii) Certificate and Key Management—

(a) To ensure the integrity of its digital certificates, the Certifying Authority shall ensure the use of approved security controls in the certificate management processes,

i.e., certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival.

(b) The method of verification of the identity of the applicant of a Public Key Certificate shall be commensurate with the level of assurance accorded to the certificate.

(c) The Certifying Authority shall ensure the continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties.

(d) In the event of a compromise of the private key the Certifying Authority shall follow the established procedures for immediate revocation of the affected subscribers' certificates.

(e) The Certifying Authority shall make available the information relating to certificates issued and/or revoked by it to the Controller for inclusion in the National Repository.

(f) The private key of the Certifying Authority shall be adequately secured at each phase of its life cycle, i.e., key generation, distribution, storage, usage, backup, archival and destruction.

(g) The private key of the Certifying Authority shall be stored in high security module in accordance with FIPS 140-1 level 3 recommendations for Cryptographic Modules Validation List.

(h) Continued availability of the private key be ensured through approved backup measures in the event of loss or corruption of its private key.

(i) All submission of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller must ensure that subscribers and relying parties are able to access the National Repository using LDAP ver 3 for X.500 Directories.

(j) The Certifying Authority shall ensure that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller.

(iv) Systems and Operations—

(a) The Certifying Authority shall prepare detailed manuals for performing all its activities and shall scrupulously adhere to them.

(b) Approved access and integrity controls such as intrusion detection, virus scanning, prevention of denial-of service attacks and physical security measures shall be followed by the Certifying Authority for all its systems that store and process the subscribers' information and certificates.

(c) The Certifying Authority shall maintain records of all activities and review them regularly to detect any anomaly in the system.

(v) Physical, Procedural and Personnel Security—

(a) Every Certifying Authority shall get an independent periodic audit done through an approved auditor. Such periodic audits shall focus on the following issues among others :

(i) changes/additions in physical controls such as site location, access, etc.;

(ii) re-deployment of personnel from an approved role/ task to a new one;

(iii) appropriate security clearnces for outgoing employees such as deletion of keys and all access privileges;

(iv) thorough background checks, etc., during employment of new personnel.

(b) The Certifying Authority shall follow approved procedures to ensure that all the activities referred to in (i) to (iv) in sub-regulation (a) are recorded properly and made available during audits.

(vi) Financial—

(a) Every Certifying Authority shall comply with all the financial parameters during the period of validity of the licence, issued under the Act.

(b) Any loss to the subscriber, which is attributed to the Certifying Authority, shall be made good by the Certifying Authority.

(vii) Compliance Audits—

(a) The Certifying Authority shall subject itself to Compliance Audits that shall be carried out by one of the empanelled Auditors duly authorised by the Controller for the purpose. Such audits shall be based on the Internet Engineering Task Force document RFC 2527-Internet X.509 PKI 509 Certificate Policy and Certification Practices Framework.

(b) If a Digital Signature Certificate issued by the Certifying Authority is found to be fictitious or that proper identification procedures have not been followed by the Certifying Authority while issuing such certificate, the Certifying Authority shall be liable for any losses resulting out of this lapse and shall be liable to pay compensation as decided by the Controller.

4. The standards followed by the Certifying Authority for carrying out its functions—(1) Every Certifying Authority shall observe the following standards for carrying out different activities associated with its functions :

(a) PKIX (Public Key Infrastructure)

Public Key Infrastructure as recommended by Internet Engineering Task Force (IETF) document draft-ietf-pkix-roadmap-05 for "Internet X.509 Public Key Infrastructure" (March 10, 2000);

(b) Public-key cryptography based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families :

Discrete Logarithm (DL) systems
Elliptic Curve Discrete Logarithm (EC) systems
Integer Factorization (IF) systems;

(c) Public-key Cryptography Standards (PKCS)

PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
PKCS#3 Diffie-Hellman Key Agreement Standard
PKCS#5 Password Based Encryption Standard
PKCS#6 Extended-Certificate Syntax Standard
PKCS#7 Cryptographic Message Syntax Standard
PKCS#8 Private Key Information Syntax Standard
PKCS#9 Selected Attribute Types
PKCS#10 RSA Certification Request

PKCS#11 Cryptographic Token Interface Standard
PKCS#12 Portable format for storing/transporting a user's private keys and certificates
PKCS#13 Elliptic Curve Cryptography Standard
PKCS#15 Cryptographic Token Information Format Standard;

(d) Federal Information Processing Standards (FIPS)

FIPS 180-1, Secure Hash Standard
FIPS 186-1, Digital Signature Standard (DSS)
FIPS 140-1 level 3, Security Requirement for Cryptographic Modules;

(e) Discrete Logarithm (DL) systems

Diffie-Hellman, MQV key agreement
DSA, Nyberg-Rueppel signatures;

(f) Elliptic Curve (EC) systems

Elliptic curve analogs of DL systems;

(g) Integer Factorization (IF) systems

RSA encryption
RSA, Rabin-Williams signatures;

(h) Key agreement schemes

(i) Signature schemes

DL/EC scheme with message recovery
PSS, FDH, PKCS #1 encoding methods for IF family
PSS-R for message recovery in IF family;

(ii) *Encryption schemes*

Abadalla-Bellare-Rogaway DHAES for DL/EC family;

(i) Form and size of the key pairs

(1) The minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 for the Certifying Authority's key pairs and 1024 for the key pairs used by subscribers.

(2) The Certifying Authority's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certifying Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in the approved Certificate Practice Statements are adhered to.

(3) The subscriber's key pairs shall be changed every one to two years;

(j) Directory Services (LDAP ver 3)

X. 500 for publication of Public Key Certificates and Certificate Revocation Lists

X. 509 version 3 Certificates as specified in ITF RFC 1422

X. 509 version 2 Certificate Revocation Lists;

(i) Publication of Public Key Certificate—The Certifying Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers and relying parties. The Certifying Authority shall be responsible and shall ensure the transmission of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller, for access by subscribers and relying parties. The National Repository shall conform to X.500 Directory Services and provide for access through LDAP Ver 3. The Certifying Authority shall be responsible for ensuring that Public Key Certificates and Certificate Revocation Lists integrate seamlessly with the National Repository on their transmission;

(k) Public Key Certificate Standard

All Public Key Certificates issued by the Certifying Authorities shall conform to International Telecommunication Union X. 509 version 3 standard. X. 509 v 3 certificate basic syntax is as follows—

TBSCertificate

{

Version	
Serial Number	
Signature	
Issuer	
Validity	
Subject	
Subject Public Key Information	
Issue Unique ID [1]	IMPLICIT Unique Identifier *optional*, —If present, version shall be v2 or v3
Subject Unique ID [2]	IMPLICIT Unique Identifier *optional*, —If present, version shall be v2 or v3
Extensions [3]	EXPLICIT Extensions *optional* —If present, version shall be v3

{
Authority Key Identifier
{
Key Identifier *optional,*
Authority Certificate Issuer *optional,*
Authority Certificate Serial Number *optional*
}
Subject Key Identifier
Key Usage
{
Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Key Cert Sign
cRLSign
Encipher Only
Decipher Only
}
Private Key Usage Period
Not Before *optional,*
Not After *optional*
{
Certificate Policies
{
Policy Information
{
Policy Identifier
Policy Qualifiers *optional*
}
Certificate Policy Id
{
Policy Qualifier Info
{
Policy Qualifier Id
Qualifier
{
cPSuri
User Notice

```
            {
              Notice Reference optional
              {
                Organisation
                Notice Numbers
              }
              Display Text optional
              {
                visibleString
                bmpString
                utf8String
              }
Policy Mappings
{
   Issuer Domain Policy
   Subject Domain Policy
}
Subject Alternative Name
{
   General Name
   {
      Other Name
      {
        type-id
        value
      }
        Rfc822Name
        DNS Name
        X400 Address
        Directory Name
        edi Party Name
        {
          Name Assigner optional,
          Party Name
        }
        Uniform Resource Identifier
        IP Address
        Registered ID
   }
}
```

Issuer Alternative Names
Subject Directory Attributes
Basic Constraints
{
cA
path Len Constraint *optional*
}
Name Constraints
{
Permitted Subtrees *optional*
Excluded Subtrees *optional*
}
Policy Constraints
{
Require Explicit Policy *optional*
Inhibit Policy Mapping *optional*
}
Extended key usage field
{
Extended Key Usage Syntax
Key Purpose Id
{
Server Authentication
Client Authentication
Code Signing
Email Protection
Time Stamping
}
}
CRL Distribution Points
{
CRL Distribution Points Syntax
Distribution Point
{
Distribution Point *optional*
{
full Name
name Relative To CRL Issuer
}
}

Reasons *optional*
{
Unused
Key Compromise
CA Compromise
Affiliation Changed
Superseded
Cessation Of Operation
Certificate Hold
}
cRL Issuer *optional*
}
Authority Information Access
{
Authority Information Access Syntax
Access Description
{
Access Method
Access Location
}
}
Signature Algorithm
Signature Value
}

(i) Certificate—TBSCertificate "to be signed". The field contains the name of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The fields are described in detail.

(ii) Version—This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, use X.509 version 3 (value is 2). If no extensions are present, but a Unique Identifier is present, use version 2 (value is 1). If only basic fields are present, use version 1 (the value is omitted from the certificate as the default value).

(iii) Serial Number—The serial number is an integer assigned by the Certifying Authority to each certificate. It shall be unique for each certificate issued by a given Certifying Authority (i.e., the issuer name and serial number identify a unique certificate).

(iv) Signature—This field contains the algorithm identifier

for the algorithm used by the Certifying Authority to sign the certificate.

(v) Issuer—The issuer field identifies the entity who has signed and issued the certificate. The issuer field shall contains a non-empty distinguished name.

(vi) Validity—The certificate validity period is the time interval during which the Certifying Authority warrants that it will maintain information about the status of the certificate.

(vii) Subject—The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name may be carried in the subject field and/or subjectAltName extension. If the subject is a Certifying Authority (e.g., the basic constraints extension, is present and the value of cA is TRUE,) then the subject field shall be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject Certifying Authority.

(viii) Subject Public Key Information—This field is used to carry the public key and identify the algorithm with which the key is used.

(ix) Unique Identifiers—These fields may only appear if the version is 2 or 3. The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time.

(x) Extensions—This field may only appear if the version is 3. The extensions defined for X.509 v3 certificates provides methods for associating additional attributes with users or public keys and for managing the certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. If present, this field is a sequence of one or more certificate extensions. The content of certificate extensions in the Internet Public Key Infrastructure is defined as follows, namely :

(a) Authority Key Identifier—The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the

subject key identifier in the issuer's certificate) or on the issuer name and serial number.

(b) Subject Key Identifier—The subject key identifier extension provides a means of identifying certificates that contain a particular public key.

(c) Key Usage—The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted. For example, when as RSA key should be used only for signing, the Digital Signature and/or non-Repudiation bits would be asserted. Likewise, when an RSA key should be used only for key management, the key Encipherment bit would be asserted.

(d) Private Key Usage Period—The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate. This extension is intended for use with digital signature keys. This extension consists of two optional components, not Before and not After. (This profile recommends against the use of this extension. Certifying Authorities conforming to this profile MUST NOT generate certificates with critical private key usage period extensions).

(e) Certificate Policies—The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Optional qualifiers, which may be present, are not expected to change the definition of the policy.

(f) Policy Mappings—This extension is used in Certifying Authority certificates. It lists one or more pairs of object identifiers; each pair includes an issuer Domain Policy and a subject Domain Policy. The pairing indicates the issuing Certifying Authority considers its issuer Domain Policy equivalent to the subject Certifying Authority's subject Domain Policy.

(g) Subject Alternative Name—The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic

mail address, a Directory Naming Service name, an IP address, and a uniform resource identifier (URI).

(h) Issuer Alternative Names—The extension is used to associate Internet style identities with the certificate issuer.

(i) Subject Directory Attributes—The subject directory attributes extension is not recommended as an essential part of this profile, but it may be used in local environments.

(j) Basic Constraints—The basic constraints extension identifies whether the subject of the certificate is a Certifying Authority and how deep a certification path may exist through that Certifying Authority.

(k) Name Constraints—The name constraints extension, which MUST be used only in a Certificate Authority Certificate, indicates a name space within which all subject names in subsequent certificates in a certification path shall be located. Restrictions may apply to the subject distinguished name or subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable.

(l) Policy Constraints—The policy constraints extension can be used in certificates issued to Certifying Authorities. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier.

(m) Extended Key Usage Field—This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.

(n) CRL Distribution Points—The CRL distribution points extension identifies how CRL information is obtained.

(o) Private Internet Extensions—This extension may be used to direct applications to identify an on-line validation service supporting the issuing Certifying Authority.

(p) Authority Information Access—The authority information access extension indicates how to access Certifying Authority information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and Certifying Authority policy data.

(xi) Signature Algorithm—The Signature Algorithm field contains the identifier for the cryptographic algorithm used by the Certifiying Authority to sign this certificate. The algorithm identifier is used to identify a cryptographic algorithm.

(xii) Signature Value—The Signature Value field contains a digital signature computed upon the Abstract Syntax Notation (ASN.1) DER encoded tbsCertificate. The ASN.1 Der encoded tbsCertificate is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate's signature field.

(xiii) Certificate Revocation List Standard—CRL and CRL Extension Profile—The CRL contents as per International Telecommunications Union standard ver 2 are as follows :

Certificate List

{

TBSCertList

{

Version

Signature

Issuer

This Update

Next Update

Revoked Certificates

{

User Certificate

Revocation Date

Certificate Revocation List Entry Extensions

{

Reason Code

{

Unspecified

Key Compromise

CA Compromise

Affiliation Changed

Superseded

Cessation Of Operation

Certificate Hold

Remove From Certificate Revocation List

}
}
Hold Instruction Code
Invalidity Date
Certificate Issuer
} *optional*
Certificate Revocation List Extension
{
Authority Key Identifier
Issuer Alternative Name
Certificate Revocation List Number
Delta Certificate Revocation List Indicator
Issuing Distribution Point
{
Distribution Point
Only Contains User Certs
Only Contains CA Certs
Only Some Reasons
Indirect Certificate Revocation List
}
} *optional*
Signature Algorithm
Signature Value
}

(i) TBSCertList : The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the Certificate Revocation List issuer, the algorithm used to sign the Certificate Revocation List, the date and time the Certificate Revocation List was issued, and the date and time by which the Certifying Authority will issue the next Certificate Revocation List.

Optional fields include lists of revoked certificates and Certificate Revocation List extension. The Revoked Certificate List is optional to support the case where a Certifying Authority has not revoked any unexpired certificates that it has issued. The profile requires conforming Certifying Authorities to use the Certificate Revocation List extension CRL Number in all Certificate Revocation Lists issued.

The first field in the sequence is the tbsCertList. This field is

itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and optional Certificate Revocation List extensions. Further, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional Certificate Revocation List entry extensions. The fields are described in detail, as follows namely—

(ii) Version—This optional field describes the version of the encoded Certificate Revocation List. When extensions are used, as required by this profile, this field MUST specify version 2 (the integer value is 1).

(iii) Signature—This field contains the algorithm identifier for the algorithm used to sign the Certificate Revocation List. This field shall contain the same algorithm identifier as the signature Algorithm field in the sequence Certificate List.

(iv) Issuer Name—The issuer name identifies the entity who has signed and issued the Certificate Revocation List. The issuer identity is carried in the issuer name field. Alternative name forms may also appear in the issuer Alternate Name extension. The issuer name field MUST contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and MUST follow the encoding rules for the issuer name field in the certificate.

(v) This Update—This field indicates the issue date of this Certificate Revocation List. This Update may be encodd-as UTC Time or Generalized Time. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists MUST encode. This Update as UTCTime for dates through the year 2049. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists MUST encode. This Update as Generalized time for dates in the year 2050 or later.

(vi) Next Update—This field indicates the date by which the next Certificate Revocation List will be issued. The next Certificate Revocation List could be issued before the indicated date, but it will not be issued any later than the indicated date. Certifying Authorities should issue Certificate Revocation Lists with a Next Update time equal to or later than all previous Certificate Revocation Lists. Next Update may be encoded as UTCTime or GeneralizedTime.

(vii) Revoked Certificates—Revoked certificates are listed. The revoked certificates are named by their serial numbers. Certificates revoked by the Certifying Authority are uniquely identified by the certificate serial number. The date on which the revocation occurred is specified. Additional information may be supplied in Certificate Revocation List entry extensions.

(viii) CRL Entry Extensions—The Certificate Revocation List entry extensions already defined by American National Standards Institute X9 and International Standards Organisation/IEC/ International Telecommunication Union for X.509 v2 Certificate Revocation Lists provide methods for associating additional attributes with Certificate Revocation List entries [X.509] [X9.55], The X.509 v2 Certificate Revocation List format also allows communities to define provide Certificate Revocation. List entry extension to carry information unique to those communities. All Certificate Revocation List entry extensions used in this specification are non-critical.

(a) Reason Code—The reason Code is a non-critical Certificate Revocation List entry extension that identifies the reason for the certificate revocation. Certifying Authorities are strongly encouraged to include meaningful reason codes in Certificate Revocation List entries; however, the reason code Certificate Revocation List entry extension should be absent instead of using the unspecified (0) Reason Code value.

(b) Hold Instruction Code—The hold instruction code is a non-critical Certificate Revocation List entry extension that provides a registered instruction identifier, which indicates the action to be taken after encountering a certificate that has been placed on hold.

(c) Invalidity Date—The invalidity date is a non-critical Certificate Revocation List entry extension that provides the date on which it is known or suspected that private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the Certificate Revocation List entry, which is the date at which the Certifying Authority processed the revocation.

(d) Certificate Issuer—This Certificate Revocation List entry extension identifies the certificate issuer associated with an entry in an indirect Certificate Revocation List, i.e., a Certificate Revocation

List that has the indirect Certificate Revocation List indicator set in its issuing distribution point extension. If this extension is not present on the first entry in an indirect Certificate Revocation List, the certificate issuer defaults to the Certificate Revocation List issuer. On subsequent entries in an indirect Certificate Revocation List, if this extension is not present, the certificate issuer for the entry is the same as that for the preceding entry.

(ix) Issuing Distribution Point—The issuing distribution point is a critical Certificate Revocation List extension that identifies the Certificate Revocation List distribution point for a particular Certificate Revocation List, and it indicates whether the Certificate Revocation List covers revocation for end entity certificates only, Certifying Authority certificates only, or a limited set of reason codes. Although the extension is critical, conforming implementations are not required to support this extension.

(x) Signature Algorithm—The signature Algorithm filed contains the algorithm identified for the algorithm used by the Certifying Authority to sign the Certificate List. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList.

(xi) Signature Value—The signature Value contains a digital signature computed upon the ASN. 1 DER encoded to be signed CerList. The ASN. 1 DER encoded tbs CertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate Revocation List's signature Value field.

(2) The list of standards specified in sub-regulation (1) shall be updated at least once a year to include new standards that may emerge from the international bodies. In addition, if any Certifying Authority or a group of Certifying Authorities brings a set of standards to the Controller for a specific user community, the Controller shall examine the same and respond to them within ninety days.

5. *Every Certifying Authority shall disclose*—(1) (a) Its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any Certification Practice Statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and

(d) any other fact that materially or adversely affect either the reliability of a Digital Signature Certificate, which that Authority has issued by it or the Authority's ability to perform its services.

(2) The above disclosure shall be made available to the Controller through filling up of online forms on the Web site of the Controller on the date and time the information is made public. The Certifying Authority shall digitally sign the information.

6. Communication of compromise of Private Key—(1) Where the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate the same without any delay to the Certifying Authority.

(2) An application for revocation of the key pair shall be made in Form online on the web site of the concerned Certifying Authority to enable revocation and publication in the Certificate Revocation List. The subscriber shall encrypt this transaction by using the public key of the Certifying Authority. The transaction shall be further authenticated with the private key of the subscriber even though it may have already been compromised.

FORM

[*See* regulation 6]

Communication of Compromise of Private Key

1. Name of Holder	:	.....
2. Public Key of Holder	:	(Attach PKC)
3. Category of Certificate	:	Individual/Organisation/ Web Server...../Other (please specify)
4. e-mail address	:	.....
5. Distinguished Name	:	.....
6. Serial No. of Certificate	:	.....
7. Certificate Fingerprint	:	.....
8. Date and Time of communication	:	.....

(Digital Signature of Holder)

Appendix 5

The Cyber Regulations Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Presiding Officer) Rules, 2003[1]

In exercise of the powers conferred by clause (s) of sub-section (2) of section 87, read with sub-section (3) of section 54 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely :

1. Short title and commencement—(1) These rules may be called the Cyber Regulations Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Presiding Officer) Rules, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these rules, unless the context otherwise requires—

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

(b) "Committee" means a Committee constituted under sub-rule (2) of rule 3;

(c) "Presiding Officer" means Presiding Officer of the Tribunal appointed under section 49 of the Act;

1. Vide G.S.R. 901 (E), dated 21st November, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

(d) "Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48 of the Act;

(e) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

3. Committee for investigation of complaints—(1) If a written complaint, alleging any definite charges of misbehaviour or incapacity to perform the functions of the offices in respect of a Presiding Officer, is received by the Central Government, it shall make a preliminary scrutiny of such complaint.

(2) If on preliminary scrutiny, the Central Government considers it necessary to investigate into the allegation, it shall place the complaint together with supporting material as may be available, before a Committee consisting of the following officers to investigate the charges of allegations made in the complaint :

(i) Secretary (Co-ordinator and Public Grievances) Cabinet Secretariat —Chairman

(ii) Secretary, Department of Information Technology —Member

(iii) Secretary, Department of Legal Affairs, Ministry of Law and Justice —Member

(3) The Committee shall devise its own procedure and method of investigation which may include recording of evidence of the complaintant and collection of material relevant to the inquiry which may be conducted by a Judge of the Supreme Court under these rules.

(4) The Committee shall submit its findings to the President as early as possible within a period that may be specified by the President in this behalf.

4. Judge to conduct inquiry—(1) If the President is of the opinion that there are reasonable grounds for making an inquiry into the truth of any imputation of misbehaviour or incapacity of a Presiding Officer, he shall make a reference to the Chief Justice of India requesting him to nominate a Judge of the Supreme Court to conduct the inquiry.

(2) The President shall, by order, appoint the Judge of the Supreme Court nominated by the Chief Justice of India

(hereinafter referred to as Judge) for the purpose of conducting the inquiry.

(3) Notice of appointment of a Judge under sub-rule (2) shall be given to the Presiding Officer.

(4) The President shall forward to the Judge a copy of—

(a) the articles of charges against the Presiding Officer concerned and the statement of imputations;

(b) the statement of witnesses, if any; and

(c) material documents relevant to the inquiry.

(5) The Judge appointed under sub-rule (2) shall complete the inquiry within such time or further time as may be specified by the President.

(6) The Presiding Officer concerned shall be given a reasonable opportunity of presenting a written statement of defence within such time as may be specified in this behalf by the Judge.

(7) Where it is alleged that the Presiding Officer concerned is unable to discharge the duties of his office efficiently due to any physical or mental incapacity and the allegation is denied, the Judge may arrange for the medical examination of the Presiding Officer by such Medical Board as may be appointed for the purpose by the President and the Presiding Officer concerned shall submit himself to such medical examination within the time specified in this behalf by the Judge.

(8) The Medical Board shall undertake such medical examination of the Presiding Officer as may be considered necessary to and submit a report to the Judge stating therein whether the incapacity is such as to render the Presiding Officer unfit to continue in office.

(9) If the Presiding Officer refuses to undergo such medical examination as considered necessary by the Medical Board, the Board shall submit a report to the Judge stating therein the examination which the Presiding Officer has refused to undergo, and the Judge may, on receipt of such report, presume that the Presiding Officer suffers from such physical or mental incapacity as is alleged in the Presiding Officer.

(10) The Judge may, after considering the written statement

of the Presiding Officer and the Medical Report, if any, amend the charges referred to in clause (a) of sub-rule (4), and in such case, the Presiding Officer shall be given a reasonable opportunity of presenting a fresh written statement of defence.

(11) The Central Government shall appoint an officer of that Government or an advocate to present the case against the Presiding Officer.

(12) Where the Central Government has appointed an advocate to present its case before the Judge, the Presiding Officer concerned shall also be allowed to present his case by an advocate chosen by him.

5. Application of the Department Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 to inquiries under these rules—The provisions of the Department Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 (18 of 1972), shall apply to the inquiries made under these rules as they apply to departmental inquiries.

6. Powers of Judge—The Judge shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and shall have power to regulate his own procedure including the fixing of places and times of his inquiry.

7. Suspension of Presiding Officer—Notwithstanding anything contained in rule 4 and without any prejudice to any action being taken in accordance with the said rule, the President, keeping in view the gravity of charges may suspend the Presiding Officer of the Tribunal against whom a complaint is under investigation or inquiry.

8. Subsistence allowance—The payment of subsistence allowance to a Presiding Officer under suspension shall be regulated in accordance with the rules and orders for the time being applicable to a Secretary to the Government of India belonging to the Indian Administrative Service.

9. Inquiry report—After the conclusion of the investigation, the Judge shall submit his report to the President stating therein his findings and the reasons therefore on each of the articles of charges seperately with such observations on the whole case as he thinks fit.

Appendix 6

The Information Technology (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules, 2003[1]

In exercise of the powers conferred by clause (v) of sub-section (2) of section 87, read with clause (g) of sub-section (2) of section 58 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:

1. Short title and commencement—(1) These rules may be called the Information Technology (Other Powers of Civil Court vested in Cyber Appellate Tribunal) Rules, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these rules, unless the context otherwise requires—

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

(b) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48 of the Act;

(c) words and expressions used herein and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

---

1. Vide G.S.R. 901 (E), dated 21st November, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

3. Powers of Cyber Appellate Tribunal—The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under the Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely :

(a) setting aside any order of dismissal of any application for default or any order pased by it, *ex parte*;

(b) requisitioning of any public record, document or electronic record from any court or office.

Appendix 7

The Information Technology (Other Standards) Rules, 2003[1]

In exercise of the powers conferred by clause (g) of sub-section (2) of section 87, read with sub-section (2) of section 20 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely :

1. Short title and commencement—(1) These rules may be called the Information Technology (Other Standards) Rules, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these rules, unless the context, otherwise requires,—

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

(b) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17 of the Act;

(c) "digital signature" means authentication of any electronic record by subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Act;

(d) words and expressions used herein and not defined but

1. Vide G.S.R. 904(E), dated 21st November, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

defined in the Act shall have the meaning respectively assigned to them in the Act.

3. Standards to be observed by the Controller—The Controller shall, observe the standards laid down in Information Technology Security Guidelines and Security Guidelines for Certifying Authorities referred to in the Information Technology (Certifying Authorities) Rules, 2000, to ensure that the secrecy and security of the digital signatures are assured.

Appendix 8

The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003[1]

In exercise of the powers conferred by clauses (p) and (q) of sub-section (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules namely :

1. Short title and commencement—(a) These rules may be called the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003.

(b) These shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these rules, unless the context otherwise requires—

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

(b) "Adjudicating Officer" means an adjudicating officer appointed under sub-section (1) of section 46 of the Act;

(c) "Proforma" means a proforma appended to these rules;

(d) words and expressions used herein and not defined but

1. Vide G.S.R. 220 (E), dated 21st November, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

defined in the Act shall have the meaning respectively assigned to them in the Act.

3. Eligibility for Adjudicating Officer—Whereas the purpose and intent of section 46 (3) of IT Act is that the Adjudicating Officer should be a person so qualified and experienced to take decisions with a view in relation to information technology aspects as well as in a position to determine the complaints keeping in view the legal or judicial mannerism on the principle of compensation of damages of IT Act.

A person shall not be qualified for appointment as Adjudicating Officer unless the person :

(a) possesses a University Graduate Bachelor Degree or equivalent, recognised by Central Government/State Government for the purpose of recruitment to Grade I Service in a Government Department through Union/ State Public Service Commission;

(b) possesses information technology experience in the areas of relevance to public interface with Central/ State Government functioning and experience obtained though the in-service training imparting competence to operate computer system to send and receive e-mails or other information through the computer network, exposure and awareness about the method of carrying information, data, sound, images or other electronic records through the medium of network including Internet;

(c) possesses legal or judicial experience to discharge responsibilities connected with the role of Central/State Government in respect of making decisions or orders in relation to administration of laws as a District Magistrate, or Additional District Magistrate or Sub-Divisional Magistrate or an Executive Magistrate or in other administrative or quasi-judicial capacity for a cumulative period of 5 years;

(d) is working and holding a post in Grade I in Government Department either in State Government/Union Territories to perform functional duty and discharge job responsibility in the field of information technology;

(e) is an in-service officer not below the rank of Director to the Government of India or an equivalent officer of State Government.

4. Secure and manner of holding inquiry—(a) The Adjudicating Officers shall exercise jurisdiction in respect of the contraventions in relation to Chapter IX of IT Act, 2000 and the matter or matters or places or area or areas in a State or Union Territory of the posting of the person.

(b) The complaint shall be made to the Adjudicating Officer of the State or Union Territory on the basis of location of Computer System, Computer Network as defined in sub-section 2 of section 75 of IT Act on a plain paper on the proforma attached to these rules together with the fee payable calculated on the basis of damages claimed by way of compensation.

(c) The Adjudicating Officer shall issue a notice together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings. The notice shall contain such particulars as far as may be as to the time and place of the alleged contravention, and the person (if any) against whom, or the thing (if any) in respect of which, it was committed.

(d) On the date so fixed, the Adjudicating Officer shall explain to such person or persons to whom notice is issued about the contravention alleged to have been committed in relation to any of the provisions of the Act or of any rule, regulation, direction or order made thereunder.

(e) If the person in respect of whom notice is issued pleads guilty, the Adjudicating Officer shall record the plea, and may impose penalty or award such compensation as he thinks fit in accordance with the provisions of the Act, rules, regulations, order or directions made thereunder.

(f) Alternatively on the date fixed the person or persons against whom a matter is filed may show cause why an enquiry should not be held in the alleged contravention or that why the report alleging the contravention should be dismissed.

(g) The Adjudicating Officer on the basis of the report of the matter, investigation report (if any), other documents and on the basis of submissions shall form an opinion that there is sufficient

cause for holding an enquiry or that the report into the matter should be dismissed and on that basis shall either by order dismiss the report of the matter, or shall determine to hear the matter.

(h) If any person or persons fails, neglects or refuses to appear, or present himself as required by sub-rule (d), before the Adjuciating Officer, the Adjudicating Officer shall proceed with the inquiry in the absence of such person or persons after recording the reasons for doing so.

(i) At any time or on receipt of a report of contravention from an aggrieved person, or by a Government agency or *suo-moto*, the Adjudicating Officer, may get the matter or the report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police, to ascertain more facts and whether *prima facie* there is a case for adjudicating on the matter or not.

(j) The Adjudicating Officer, shall fix a date and time for production of documents of evidence and for this purpose may also rely on electronic records or communications and as far as may be, shall use or make available the infrastructure for promoting on-line settlement of enquiry or disputes or for taking evidence including the services of an adjudicating officer and infrastructure in another State.

(k) As far as possible, every application shall be heard and decided in four months and the whole matter in six months.

(l) Adjudicating Officer, when convinced that the scope of the case extends to the Offence(s) (under Chapter XI of IT Act) instead of contravention, needing appropriate punishment instead of mere financial penalty, should transfer the case to the Magistrate having jurisdiction to try the case, through Presiding Officer.

5. Order of the Adjudicating Officer—(a) If, upon consideration of the evidence produced before the Adjudicating Officer and other records and submissions, the Adjudicating Officer is satisfied that the person has become liable to pay damages by way of compensation or to pay penalty under any of the provisions of the Act or rules, regulations, directions or orders,

the Adjudicating Officer may, by order in writing, order payment of damages by way of compensation or impose such penalty, as deemed fit.

(b) While adjudging the quantum of compensation or penalty, the Adjudicating Officer shall have due regard to the following factors, namely :

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

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

(iii) the repetitive nature of the default.

6. Copy of the order—Adjudicating Officers shall deliver a certified copy of the order to the complainant and respondent.

7. Service of notices and orders—A notice or an order issued under these rules shall be served on the person in any of the following manners, that is to say :

(a) by delivering or tendering it to that person or the person's authorised agent in an electronic form provided that there is sufficient evidence of actual delivery of the electronic record to the concerned person; or

(b) by sending it to the person by registered post with acknowledgement due to the address of his place of residence or the last known place of residence or business place;

(c) if it cannot be served under (a) or (b) above then by affixing it, in the presence of two witnesses, on the outer door or some other conspicuous part of the premises in which that person resides or is known to have last resided, or carried on business or personally works or last worked for gain.

8. Fee—Every complaint of a matter to the Adjudicating Officer shall be accompanied by fee, payable by a bank draft drawn in favour of "Adjudicating Officer Information Technology Act" at the place of functioning of Adjudicating Officer in the States or Union Territories, calculated on the basis of the damages claimed by way of comprehension from the contraveners on the rates provided below :

TABLE OF FEE

(I) Damages by way of compensation	Fee
(a) Up to Rs. 10,000	10% *ad valorem* rounded of to nearest next hundred.
(b) From 10001 to Rs. 50,000	Rs. 1,000 plus 5% of the amount exceeding Rs. 10,000/—rounded of to nearest next hundred.
(c) From Rs/ 50,001 to Rs. 1,00,000	Rs. 3,000/- plus 4% of the amount exceeding Rs. 50,000 rounded of to nearest next hundred.
(d) More than Rs. 10,000	Rs. 5,000/- plus 2% of the amount exceeding Rs. 1,00,000 rounded of to nearest next hundred.
(II) Fee for every application	Rs. 50/-

9. Duplicity avoided—When an adjudication into a matter of contravention is pending before an Adjudicating Officer, same matter shall not be pursued before any court or Tribunal or Authority in any proceeding whatsoever and if there is already filed a report in relation to the same matter, the proceedings before such other court, Tribunal or Authority shall be deemed to be withdrawn.

10. Frivolous complaints—If a person files a frivolous report of the matter, the Adjudicating Officer in his discretion may order the complainant, to make good the cost of the persons against whom the complaint was filed and to pay a damage of not exceeding rupees twenty-five thousand and the Adjudicating Officer may also order payment of a fine up to an amount not exceeding rupees ten thousand only.

11. Compounding of contraventions—(a) A person, against whom a report of contravention of the Act, Rules or Regulations, directions or orders or conditions has been filed before an Adjudicating Officer, may make an application for compounding the contravention during the adjudicating proceedings to the concerned Adjudicating Officer :

Provided that an application for compounding may be filed even before the contravention is reported, in which case the

contravener himself shall state the contravention undertaken or committed and the likely loss to various parties and the amount of compensatory damages tendered by the contravener.

(b) The applicant desirous of compounding the contravention shall deposit the sum determined by the office of Adjudicating Officer :

Provided that sum determined as compounding fee shall not exceed the maximum amount of penalty, which may be imposed under this Act for the contraventions so compounded.

12. Certifying Authorities and other Governmental agencies to assist—All the licensed or recognised Certifying Authorities, the Controller and other officers and agencies established under the Act and other Government agencies like CERT-IND shall promptly assist the Adjudicating Officers in any proceedings filed or pending before the Adjudicating Officers.

APPENDIX

Proforma for Complaint to Adjudicating Officer under Information Technology Act, 2000

I. 1. Name of the Complainant
   2. E-mail address
   3. Telephone No.
   4. Address for correspondence
   5. Digital Signature Certificate, if any

II. 1. Name of the Respondent
   2. E-mail address
   3. Telephone No.
   4. Address for correspondence
   5. Digital Signature Certificate, if any

III. Damages claimed
   Fee deposited
   Demand Draft No. ..... dated.....Branch.....

IV. Complaint under Section/Rule/Direction/Order, etc.

V. Time of Contravention

VI. Place of Contravention

VII. Cause of action

VIII. Brief facts of the case

Signature of the Complainant

Appendix 9

The Cyber Regulations Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Presiding Officer) Rules, 2003[1]

In exercise of the powers conferred by clause (r) of sub-section (2) of section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the terms and conditions of the service of the Presiding Officer, namely :

1. Short title and commencement—(a) These rules may be called the Cyber Regulations Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Presiding Officer) Rules, 2003.

(b) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions—In these rules, unless the context otherwise requires—

(a) "Cyber Appellate Tribunal" means Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(b) "Presiding Officer" means a person appointed as Presiding Officer of a Cyber Appellate Tribunal under section 49 of the Act;

1. Vide G.S.R. 221 (E), dated 17th March, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

(c) words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Salary and allowances—The Presiding Officer shall be paid such salary and allowances, as admissible to a Secretary to the Government of India, including all the benefits that a Secretary is entitled to. The Presiding Officer shall be deemed to be public servant as per the section 82 of Information Technology Act, 2000 (21 of 2000) :

Provided that in the case of appointment of a person as Presiding Officer, who has retired as a Judge of a High Court or who has retired from service under the Central Government or a State Government and who is in receipt of, or has received, or has become entitled to receive any retirement benefits by way of pension, gratuity, employer's contribution to the Provident Fund or other forms of retirement benefits, the pay of such Presiding Officer shall be reduced by the gross amount of pension or employer's contribution to the Provident Fund or any other form of retirement benefit, if any, drawn or to be drawn by him :

Provided further that in case a retired Judge of a High Court is appointed as Presiding Officer, the terms the conditions of service of such Presiding Officer shall be in accordance with the instructions issued by the Ministry of Finance in respect of appointment of Judges to various Tribunals and in consultation with that Ministry.

4. Leave—A person, on appointment as a Presiding Officer in a Cyber Appellate Tribunal shall be entitled to leave as applicable to the Secretary to the Government of India in respect of Earned Leave, Half Pay Leave, Extra Ordinary Leave, Commutation of Leave, Casual Leave, etc.

5. Leave sanctioning authority—The Secretary, Department of Information Technology, Government of India, shall be the authority competent to sanction leave to the Presiding Officer.

6. Pension or Provident Fund—(i) In case a serving Judge of a High Court or a member of the Indian Legal Service is holding the post of Presiding Officer, the service rendered in the Cyber Appellate Tribunal shall count for pension, to be drawn in accordance with the rules of the service to which he belongs, and

he shall also be governed by the provisions of the Provident Fund (Central Services) Rules, 1960.

(ii) In all other cases, the Presiding Officer shall be governed by the provisions of the Provident Fund (India) Rules, 1962.

7. Travelling allowances—The Presiding Officer while on tour (including the journey undertaken on the expiry of his term with the Cyber Appellate Tribunal to proceed to his home town) shall be entitled to the travelling allowances, daily allowances, transportation of personal effects and other similar matters at the same scales and at the same rates as are applicable to Secretary to the Government of India.

8. Leave Travel Concession—The Presiding Officer shall be entitled to avail leave travel concession as admissible to the Secretary to the Government of India.

9. Facility of conveyance—The Presiding Officer shall be entitled to hire a taxi on whole time basis in accordance with the rules or orders for the time being in force for hire of taxi by a Secretary to the Government of India.

10. Accommodation—(a) The Presiding Officer shall be eligible, subject to availability, allotment of Government Quarter from the general pool accommodation of the type admissible to a Group 'A' officer of the Central Government, who is working at the place where the Cyber Appellate Tribunal is located and drawing an equivalent pay, on payment of license fee at the rates specified by the Central Government from time to time.

(b) Where the Presiding Officer occupies a Government accommodation beyond permissible period, he shall be liable to pay additional license fee or, and he shall be liable to eviction in accordance with the rules applicable to Central Government servants.

(c) Where the Presiding Officer does not avail of facility of Government accommodation under sub-rule (a), he shall be entitled to House Rent Allowance as admissible to Group 'A' officers of the Central Government drawing equivalent pay.

11. Facilities for medical treatment—The Presiding Officer shall be entitled to medical treatment and hospital facilities, as provided in the Central Government Health Scheme Rules, 1954 and in places where the Central Government Health Scheme is

not in operation, the said Presiding Officer shall be entitled to the facilities as provided in the Central Services (Medical Attendance) Rules, 1944.

12. Residuary provision—Matters relating to the conditions of service of the Presiding Officer with respect to which no express provision has been made in these rules shall be as per the rules applicable to Group 'A' officers of Central Government.

Appendix 10

Blocking of Websites[1]

Ministry of Communication and Information Technology
(Department of Information Technology)

Order

New Delhi, 7th July, 2003

Subject : Procedure for Blocking of Websites

As per the Gazette Notification (Extraordinary) No. G.S.R. 181 (E), dated 27th February, 2003, published in Part II, Section 3, Sub-section (i), Indian Computer Emergency Response Team (CERT-In) has been designated as the single authority for issuing of instructions in the context of blocking of websites. CERT-In has to instruct the Department of Telecommunications to block the website after,

(i) verifying the authenticity of the complaint;

(ii) satisfying that action of blocking of website is absolutely essential.

II. The blocking of website may be the need of several agencies engaged in different walks of public and administrative lives due to a variety of reasons. Explicit provisions for blocking of the website in the IT Act, 2000 is available only in section 67, relating to pornographic content on the website. In addition, section 69 empowers the Controller of Certifying Authorities to intercept any information transmitted through any computer resource in relation only to the following five purposes :

1. *Vide* G.S.R. 529 (E), dated 7th July, 2003 published in the Gazette of India, Extra, Pt. II, Sec. 3(i) dated 27th November, 2003.

(i) Interest of the sovereignty or integrity of India,
(ii) The security of the State;
(iii) Friendly relations with foreign States, or
(iv) Public order, or
(v) For preventing incitement to the commission of any cognisable offence.

III. As already noted there is no explicit provision in the IT Act, 2000 for blocking of websites. In fact, blocking is taken to amount to censorship. Such blocking can be challenged if it amounts to restriction of freedom of speech and expression. But websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.

IV. The websites promoting the above mentioned types of content, not covered under the Freedom of Speech may need to be blocked under the inherent powers of the Government, "to the extent of executive authority read with legal powers vested in Central Government and Controller under various provisions of various laws".

V. The detailed procedure for submitting a complaint to the Director, CERT-In for blocking of a website shall be as follows :

1. The following officers listed in Para 2 of the Gazette Notification can submit the complaint to the Director, CERT-In :
   (i) Secretary, National Security Council Secretariat (NSCS);
   (ii) Secretary, Ministry of Home Affairs, Government of India;
   (iii) Foreign Secretary in the Department of External Affairs or a representative not below the rank of Joint Secretary;
   (iv) Secretaries, Department of Home Affairs of each of the States and of the Union Territories;
   (v) Central Bureau of Investigation (CBI), Intelligence

Bureau (IB), Director General of Police of all the States and such other enforcement agencies;

(vi) Secretaries or Heads of all the Information Technology Department of all the States and Union Territories not below the rank of Joint Secretary of Central Government;

(vii) Chairman of the National Human Rights Commission or Minorities Commission or Scheduled Tribes Commission or National Women Commission;

(viii) The directive of the Courts;

(ix) Any others as may be specified by the Government.

2. The complaint shall contain the following :

(i) Name of the complaint with address, telephone number, fax number, and e-mail.

(ii) The address of the offending website.

(iii) The name of the organisation with address, if known, which is promoting/hosting the website.

(iv) Specify reasons for requesting blocking of websites. This may be from any of the following :

Promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, promoting pornography, including child pornography and violent sex.

(v) Any other reasons may be specified by the complainant.

(vi) Segment of population or the audience that is adversely affected by the offending website.

3. The complaint may be submitted in writing by an authorised officer of the above named organisation on the letter head. This can be sent either by mail or by fax or by e-mail digitally signed.

4. Each complaint shall be assigned a complaint number and recorded in a register along with the time and date of the receipt.

5. CERT-In staff shall verify that the complainant belongs to one of the organisations that have been listed above. If needed, this will be verified telephonically from the concerned office.

6. Each complaint shall be acknowledged to the complainant within 24 hours of its receipt.
7. In the case of complaints received by fax and e-mail which is not digitally signed, the complainant shall be required to provide an ink-signed copy of the complaint so as to reach CERT-In within 3 days of the receipt of the complaint by fax or e-mail. The processing of the complaint shall begin without waiting for the receipt of the ink-signed copy.
8. Director, CERT-In will assign the complaint to a technical expert to view the said website and print the offending content as a sample within a day of the receipt of the complaint.
9. The complaint along with the printed sample content of the website shall be examined by a duly constituted committee under the chairmanship of Director, CERT-In with representatives of DIT and Law Ministry/Home Ministry. The committee will meet within a day of the complaint and the content being notified by Director, CERT-In to the members of the Committee. It will meet and take on the spot decision on whether the website is to be blocked or not.
10. The decision on blocking of the website by the Committee along with the complaint and details thereof shall be submitted by Director, CERT-In to the Additional Secretary, DIT for the approval of the Secretary, DIT.
11. On receipt of the approval from DIT, Director, CERT-In will issue instructions to DOT for blocking of website.
12. The entire exercise shall be completed within seven working days of the receipt of a complaint.
13. In case of an emergency situation, to be decided by Director, CERT-In in consultation with the Additional Secretary, DIT, instructions for blocking of website will be immediately issued by Director, CERT-In to DOT.
14. Strict confidentiality shall be maintained by CERT-In regarding all the complaints as also their processing.
15. The Director, CERT-In shall maintain complete record, in electronic database as also in paper files/registers, of the cases of blocking of website processed. This database

shall be the property of the DIT and shall not be used for any commercial purpose.

16. The Director, CERT-In shall submit a monthly report of the cases of blocking of the website processed in each month, by 7th of the next month (or the next working day if 7th happens to be a holiday), to the Additional Secretary, DIT.
17. The Director CERT-In shall arrange to make available the record of the cases of blocking of the website processed by CERT-In, as and when required for audit by an officer designated by Secretary, DIT for this purpose. This inspection/audit may be undertaken on a quarterly basis.
18. The service for blocking of the website containing offending material is to be provided by CERT-In in public interest and hence no fees shall be charged for providing this service.

Appendix 11

Glossary of Cyber Terms

A

Accept (A Digital Signature Certificate) : To demonstrate approval of a Digital Signature Certificate by a applicant while knowing or having notice of its informational contents.

Access : Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Access Control : Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL) : A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service : A security service that provides protection of system resource against unauthorised access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access : Management is the maintenance of access information which consists of four tasks : account administration, maintenance, monitoring and revocation.

Access Matrix : An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting : Account Harvesting is the process of collecting all the legitimate account names on a system.

ACK Piggybacking : ACK piggybacking is the practice of sending an ACK inside another packet going to the same destination.

Accreditation : A formal declaration by the Controller that a particular information system, professional or other employee or contractor, or organisation is approved to perform certain duties and to operate in specific security mode, using a prescribed set of safeguards.

Active Content : Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS).

Activity Monitors : Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Authority Revocation List (ARL) : A list of revoked Certifying Authority Certificates. An ARL is a CRL for Certifying Authority cross certificates.

Addressee : A person who is intended by the originator to receive the electronic record but does not include any intermediary.

Address Resolution Protocol (ARP) : Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognised in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standards (AES) : An encryption standard being developed by NIST. Intended to specify an unclassified, publicly disclosed, symmetric encryption algorithm.

Affiliated Certificate : A certificate issued to an affiliated individual.

Affirm/ Affirmation : To state or indicate by conduct that data is correct or information is true.

Affixing Digital Signature : With its grammatical variations and cognate expressions means adoption of any methodology or

procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

Algorithm : A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Alias : A pseudonym.

Applet : Java programs; an application program that uses the client's web browser to provide a user interface.

Applicant : (*See* CA applicant; certificate applicant).

Application Software : A software that is specific to the solution of an application problem. It is the software coded by or for an end user that performs a service or relates to the user's work.

Application System : A family of products designed to offer solutions for commercial data processing, office, and communication environments, as well as to provide simple, consistent programmer and end user interfaces for business of all sizes.

Archive : To store records and associated journals for a given period of time for security, backup, or auditing purposes.

Arpanet : Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Assurances : Statements or conduct intended to convey a general intention, supported by a good-faith effort, to provide and maintain a specified service. "Assurances" does not necessarily imply a guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties, unless otherwise expressly indicated.

Asymmetric Cryptography : Public key cryptography; a modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric Crypto System : A system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Asymmetric Warfare : Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

Auditing : Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Audit Trail : A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

Authenticated Record : A signed document with appropriate assurances of authentication or a message with a digital signature verified by a relying party. However, for suspension and revocation notification purposes, the digital signature contained in such notification message must have been created by the private key corresponding to the public key contained in the Digital Signature Certificate.

Authentication : Authentication is the process of confirming the correctness of the claimed identity.

Authenticity : Authenticity is the validity and conformance of the original information.

Authorization : Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System : One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Availability : Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

B

Backdoor : A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

Backup : The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

Bandwidth : Commonly used to mean the capacity of a

communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

Banner : A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorised use.

Basic Authentication : Basic Authentication is the simplest web-based authentication scheme that works by sending the user name and password with each request.

Bastion Host : A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

Bind : BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

Biometrics : Biometrics use physical characteristics of the users to determine access.

Bit : The smallest unit of information storage; a contraction of the term 'binary digit'; one of two symbols '0' (zero) and '1' (one) that are used to represent binary numbers.

Block Cipher : A block cipher encrypts one block of data at a time.

Boot Record Infector : A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

Border Gateway Protocol (BGP) : An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

Bridge : A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet of token ring).

British Standard 7799 : A standard code of practice and provides guidance on how to secure an information system. It includes the management framework, objectives and control requirements for information security management systems.

Broadcast : To simultaneously send the same message to multiple recipients. One host to all hosts on network.

Broadcast Address : An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

Browser : A client computer program that can retrieve and display information from servers on the World Wide Web.

Brute Force : A cryptanalysis technique or other kind of attack method involving an exhaustive procedures that tries all possibilities, one-by-one.

Buffer Overflow : A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Business Continuity Plan (BCP) : A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Bulletin Board Service (BBS) : A kind of service available on internet that allows a person to read the message left by other.

Business Impact Analysis (BIA) : A Business Impact Analysis determines what levels of impact to a system are tolerable.

Byte : A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.

C

Cache : Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers : memory caching and disk caching.

Cache Cramming : Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning : Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Cell : A cell is a unit of data transmitted over an ATM network.

Central Processing Unit (CPU) : A part of computer which stores and runs software.

Certificate : A Digital Signature Certificate issued by Certifying Authority.

Certificate-Based Authentication : Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

Certificate Chain : An ordered list of Certificates containing an end-user subscriber certificate and Certifying Authority certificates (*See* valid certificate).

Certificate Class : A Digital Signature Certificate of a specified level of trust.

Certificate Expiration : The time and date specified in the Digital Signature Certificate when the operational period ends, without regard to any earlier suspension or revocation.

Certificate Extension : An extension field to a Digital Signature Certificate which may convey additional information about the public key being certified, the certified subscriber, the Digital Signature Certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8 : 1995 (X. 509). Custom extension can also be defined by communities of interest.

Certificate Issuance : The actions performed by a Certifying Authority in creating a Digital Signature Certificate and notifying the Digital Signature applicant (anticipated to become a subscriber) listed in the Digital Signature Certificate of its contents.

Certificate Management [Management of Digital Signature Certificate] : Certificate management includes, but is not limited to, storage, distribution dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital Signature Certificates. A Certifying Authority undertakes Digital Signature Certificate management functions by serving as a registration authority for subscriber Digital Signature Certificates. A Certifying Authority designates issued and accepted Digital Signature Certificates as valid by publication.

Certificate Policy : A specialised form of administrative policy tuned to electronic transactions performed during Digital Signature Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Revocation : (*See* Revoke a Certificate)

Certificate Revocation List (CRL) : A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital Signature Certificates' serial numbers, and the specific times and reasons for suspension and revocation.

Certificate Serial Number : A value that unambiguously identifies a Digital Signature Certificate generated by a Certifying Authority.

Certificate Signing Request (CSR) : A machine-readable form of a Digital Signature Certificate application.

Certificate Suspension : (See Suspend a Certificate)

Certification/Certify : The process of issuing a Digital Signature Certificate by a Certifying Authority.

Certifying Authority (CA) : A person who has been granted a licence to issue a Digital Signature Certificate under section 24 of Information Technology Act, 2000.

Certifying Authority Software : The cryptographic software required to manage the keys of end entities.

Certifying Authority System : All the hardware and software system (e.g., Computer, PKI servers, network devices, etc.) used by the Certifying Authority for generation, production, issue and management of Digital Signature Certificate.

Certification Practice Statement (CPS) : A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates.

Certifier : (*See* issuing authority).

Chain of Custody : Chain of Custody is the important application of the Federal rules of evidence and its handling.

Challenge-Handshake Authentication Protocol (CHAP) : The Challenge-Handshake Authentication Protocol uses a challenge/ response authentication mechanism where the response varies every challenge to prevent replay attacks.

Challenge Phrase : A set of numbers and/or letters that are chosen by a Digital Signature Certificate applicant, communicated to the Certifying Authority with a Digital Signature Certificate application, and used by the Certifying Authority to authenticate the subscriber for various purposes as required by the Certification Practice Statement. A challenge phrase is also used by a secret share holder to authenticate himself, or itself to a secret share issuer.

Checksum : A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

Cipher : A cryptographic algorithm for encryption and decryption.

Ciphertext : Ciphertext is the encrypted form of the message being sent.

Circuit Switched Network : A circuit switched network is where a single continuous physical circuit connected two endpoints where the route was immutable once set up.

Client : A system entity that requests and uses a service provided by another system entity, called a 'server'. In some cases, the server may itself be a client of some other server.

Client Application : An application that runs on a personal computer or workstation and relies on a server to perform some operation.

Collision : A collision occurs when multiple systems transmit simultaneously on the same wire.

Common Key : Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, 'common key' refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

Communication/Network System : A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities (covering ISDN, lease lines, dial-up, LAN, WAN, etc.)

Competitive Intelligence : Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

Compromise : A violation (or suspected violation) of security policy, in which an unauthorised disclosure of, or loss of control over, sensitive information may have occurred. (*Cf.*, data integrity).

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

Computer Centre : (*See* Data Centre)

Computer Counterfeiting : It is an act of counterfeiting any valuable document or data or programme etc.

Computer Data Base : Means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

Computer Emergency Response Team (CERT) : An organisation that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Network : A collection of host computers together with the sub-network or inter-network through which they can exchange data.

Computer Peripheral : Means equipment that works in conjunction with a computer but is not a part of the main computer itself, such as printer, magnetic tape reader, etc.

Computer Resources : Means computer, computer system, computer network, data computer database or software.

Computer Sabotage : An act of criminal destruction of computer network or data or theft of valuable information stored in computer for any unlawful gain.

Computer System : A device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Computer Virus : (*See* Virus)

Confidentiality : Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.

Configuration Management : Establish a known baseline condition and manage it.

Confirm : To ascertain through appropriate inquiry and investigation. (*See also* authentication; verify a digital signature)

Confirmation of Digital Signature Certificate Chain : The process of validating a Digital Signature Certificate chain and subsequently validating an end-user subscriber Digital Signature Certificate.

Contingency Plans : The establishment of emergency response, back up operation, and post-disaster recovery processes maintained by an information processing facility or for an information system.

Establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification and priority of what must be done, who performs the required action, and what tools must be used.

A document, developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations such as disasters. Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

Cookie : Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.

Cost Benefit Analysis : A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

Controls : Measures taken to ensure the integrity and quality of a process.

Convert Channels : Convert Channels are the means by which information can be communicated between two parties in a convert fashion using normal system operations. For example, by changing the amount of hard drive space that is available on a file server can be used to communicate information.

Corruption : A threat action that undesirably alters system operation by adversely modifying system functions or data.

Correspond : To belong to the same key pair. (*See* also public key; private key)

Cracking : An act of deleting files or putting a virus or cell information or steal some source code and use for own benefits.

Critical Information : Data determined by the data owner as mission critical or essential to business purposes.

Cron : Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

Cross-Certificate : A Certificate used to establish a trust relationship between two Certifying Authorities.

Crossover Cable : A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

Cryptanalysis : The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

Cryptographic Algorithm or Hash : An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms. A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

Cryptography : Cryptography garbles a message in such a way that anyone who intercepts the message cannot understand it.

Cyber Space : The virtual location within which electronic activities take place.

Cyber Crime : An act that covers the entire range of crime which involves computer, computer networks, cell phones, etc.

Cyber Squatting : It is an act in which the site names in the internet are blocked and than traded by unscrupulous persons for unlawful gain.

Cyber Stalking : It involves repeated threat and harassment of a victim through e-mail, chat message or web pages.

Cut-Through : Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

Cyclic Redundancy Check (CRC) : Sometimes called 'cyclic redundancy code'. A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

D

Daemon : A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called by

other names. Windows, for example, refers to daemons and System Agents and services.

Damage : Means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Data : Means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Data Aggregation : Data Aggregation is the ability to get a more complete picture of the information by analysing several different types of records at once.

Data Base : (See Computer Database)

Data Centre (as also Computer Centre) : The facility covering the computer room, media library, network area, server area, programming and administration areas, other storage and support areas used to carry out the computer processing functions. Usually refers to the computer room and media library.

Data Confidentiality : (*See* Confidentiality)

Data Custodian : A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibilities for the data.

Data Encryption Standard (DES) : A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Integrity : A condition in which data has not been altered or destroyed in an unauthorised manner. (*See* also threat; compromise).

Data Mining : Data Mining is a technique used to analyse existing information, usually with the intention of pursuing new avenues to pursue business.

Data Owner : A Data Owner is the entity having responsibility and authority for the data.

Data Security : The practice of protecting data from accidental or malicious modification, destruction, or disclosure.

Data Warehousing : Data Warehousing is the consolidation of several previously independent databases into one location.

Datagram : Request for Comment 1594 says, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless).

Decapsulation : Decapsulation is the process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

Decryption : Decryption is the process of transforming an encrypted message into its original plaintext.

Defacement : Defacement is the method of modifying the content of a website in such a way that it becomes "vandalised" or embarrassing to the website owner.

Defense In-Depth : Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

Demo Certificate : A Digital Signature Certificate issued by a Certifying Authority to be used exclusively for demonstration and presentation purposes and not for any secure or confidential communications. Demo Digital Signature Certificates may be used by authorised persons only.

Denial of Service : The prevention of authorised access to a system resource or the delaying of system operations and functions.

Dictionary Attack : An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to brute force attack that tries all possible combinations.

Diffie-Hellman : A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operation, or for any other cryptography.

Digest Authentication : Digest Authentication allows a web client to compute MD5 hashes of the password to prove it has the password.

Digital Certificate : A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Certificate Applicant : A person that requests the issuance of a public key Digital Signature Certificate by a Certifying Authority. (*See* also C.A. applicant; subscriber)

Digital Certification Application : A request from a Digital Signature Certificate applicant (or authorised agent) to a Certifying Authority for the issuance of a Digital Signature Certificate. (*See also* Certificate Applicant; Certificate Signing Request)

Digital Envelope : A digital envelope is an encrypted message with the encrypted session key.

Digital Signature : A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Digital Signature Algorithm (DSA) : An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Certificate : Means a Digital Signature Certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000.

Digital Signature Standard (DSS) : The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Disassembly : The process of taking a binary program and deriving the source code from it.

Disaster Recovery Plan (DRP) : A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

Discretionary Access Control (DAC) : Discretionary Access Control consists of something the user can manage, such as a document password.

Disruption : A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Distance Vector : Distance vectors measure the cost of routes to determine the best route to all known networks.

Distinguished Name : A set of data that identifies a real-world entity, such as a person in a computer-based context.

Distributed Scans : Distributed Scans are scans that use multiple source addresses to gather information.

DNS spoofing : An act in which face nots masks are made during the resolution of internet hots names.

Document : A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information. (*See* also Message; Record)

Domain : A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Name : A domain name locates an organisation or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organisation or entity (in this example, "organisation") and is called the top-level domain name. The "sans" part of the domain name defines the organisation or entity and together with the top-level is called the second-level domain name.

Domain Hijacking : Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name System (DNS) : The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember 'handle' for an Internet address.

Due Care : Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

Due Diligence : Due diligence is the requirement that organisations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

DumpSec : DumpSec is a security tool that dumps a variety of information about a system's users, file system, registry, permission, password policy, and services.

Dumpster Diving : Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

Dynamic Link Library : A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

Dynamic Routing Protocol : Allows network devices to learn routes. Ex. RIP, EIGRP Dynamic routing occurs when routers talk to adjacent routers, informing each other of what networks each router is currently connected to. The routers must communicate

using a routing protocol, of which there are many to choose from. The process on the router that is running the routing protocol, communicating with its neighbour routers, is usually called a routing daemon. The routing daemon updates the kernel's routing table with information it receives from neighbour routers.

E

Eavesdropping : Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to facility or network.

Echo Reply : An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request : An echo request is an ICMP message sent to machine to determine if it is online and how long traffic takes to get to it.

Egrees Filtering : Filtering outbound traffic.

E-mail spoffing : A spoofed e-mail is one that appears to originate from one source but actually sent from another source.

Emanations Analysis : Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Electronic Form : With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro-film, computer generated micro fiche or similar device.

Electronic Mail (e-mail) : A method of transmission of message over communication network.

Electronic Record : Means data, record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer generated micro-fiche.

Encapsulation : The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Electronic Data Interchange (EDI) : It is a standard format used for exchange of business data.

Encryption : Cryptographic transformation of data (called

'plaintext') into a form (called 'cipher text') that conceals the data's original meaning to prevent it from being known or used.

Ephemeral Port : Also called a transient port or a temporary port. Usually is on the client side. It is set up when a client application wants to connect to a server and is destroyed when the client application terminates. It has a number chosen at random that is greater than 1023.

Electronic Evidence: Any computer generated data, including e-mail, text documents, spreadsheets, images, database, files, deleted e-mails, files, etc.

Escrow Passwords : Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

Ethernet : The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

Event : An event is an observable occurrence in a system or network.

Exponential Backoff Algorithm : An exponential backoff algorithm is used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

Exposure : A threat action whereby sensitive data is directly released to an unauthorised entity.

Extended ACLs (Cisco) : Extended ACLs are a more powerful form of Standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

Extensible Authentication Protocol (EAP) : A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

Exterior Gateway Protocol (EGP) : A protocol which distributes routing information to the routers which connect autonomous systems.

Extensions : Extension fields in X.509 v3 certificates. (*See* X.509)

Extranet : It is a network in which web and internet technologies are used in order to connect two or more business enterprises and their intranet for business communications.

F

False Rejects : False Rejects are when an authentication system fails to recognise a valid user.

Fast File System : The first major revision to the Unix file system, providing faster read access and faster (delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fault Line Attacks : Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP) : A TCP/IP protocol specifying the transfer of text or binary files across the network.

Filter : A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Filtering Router : An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forwad it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

Finger : A protocol to lookup user information on a given host. A Unix program that takes an e-mail address an input and returns information about the user who owns that e-mail address. On some systems, finger only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course,

the user must first enter this information into the system. Many e-mail programs now have a finger utility built into them.

Fingerprinting : Sending strange packets to a system in order to gauge how it responds to determine the operating system.

Firewall : A logical or physical discontinuity in a network to prevent unauthorised access to data or resources.

Flooding : An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input the entity can process properly.

Forest : A forest is a set of Active Directory domains that replicate their databases with each other.

Fork Bomb : A Fork Bomb works by using the fork () call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Form-Based Authentication : Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Forward Lookup : Forward lookup uses an Internet domain name to find an IP address.

Forward Proxy : Forward Proxies are designed to be the server through which all requests are made.

Fragment Offset : The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

Fragment Overlap Attack : A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

Fragmentation : The process of storing a data file in several 'clunks' or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Frames : Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and

contains a header field and a trailer field that 'frame' the data. (Some control frames contain no data).

Full Duplex : A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

Fully-Qualified Domain Name : A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain name.

Function : In relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

G

Gateway : A network point that acts as an entrance to another network.

gethostbyaddr : The gethostbyaddr DNS query is when the address of a machine is known and the name is needed.

gethostbyname : The gethostbyname DNS quest is when the name of a machine is known and the address is needed.

Geneate A Key Pair : A trustworthy process of creating private keys during Digital Signature Certificate application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital Signature Certificate application in a manner that demonstrates the applicant's capacity to use the private key.

GNU : GNU is a Unix-like operation system that comes with source code that can be copied, modified, and redistributed. The GNU project was started in 1983 by Richard Stallman and others, who formed the Free Software Foundation.

Gnutella : An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

H

Hard Copy : A copy of computer output that is printed on paper in a visually readable from; e.g., printed reports, listing, and documents.

Handshake (3-way Handshake) : Machine A sends a packet with a SYN flag set to Machine B. B acknowledges A's SYN with a SYN/ACK. A acknowledges B's SYN/ACK with an ACK.

Hacking : An act of penetration of computer system by may of manipulation, sabotage or espionage.

Hardening : Hardening is the process of identifying and fixing vulnerabilities on a system.

Hash Function : An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Header : A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack : A form of active wiretapping in which the attacker seizes control of a previously established communication association.

High-Security Zone : An area to which access is controlled through an entry point and limited to authorised, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day a week by security staff, other personnel or electronic means.

Hoax : It is only a false warning regarding existence of malacious programme.

Honey pot : Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Hops : A hop is each exchange with a gateway a packet takes on its way to the destination.

Host : Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that servers the pages for one or more Web sites.

Host-based ID : Host-based intrusion detection systems use information from the operating system audit records to watch all

operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilised by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTTP Proxy : An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

HTTPS : When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Hub : A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

Hybrid Attack : A Hybrid Attack builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid Encryption : An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Hyperlink : In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by colour or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link.

Hypertext Markup Language (HTML) : The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

Hypertext Transfer Protocol (HTTP) : The protocol in the Internet Protocol (IP) family used to transport hypertext documents acros an internet.

I

Identification/Identify : The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates.

Identity : Identity is who someone or what something is, for example, the name by which something is known.

ICCNN : An international self-governed organisation which performs the responsibility of internet protocol (IP).

Incident : An incident is an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling : Incident Handling is an action plan for dealing with intrusions, cyber-theft, denail of service, fire, floods, and other security-related events. It is comprised of a six step process : Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Icremental Backups : Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

Inetd (xinetd) : Inetd (or Internet Daemon) is an application that controls smaller internet services like telnet, ftp, and POP.

Inference Attack : Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

Ingress Filtering : Ingress Filtering is filtering inbound traffic.

Interrupt : An Interrupt is a signal that informs the OS that something has occurred.

Information : Includes data, images, sound, voice, codes, computer programs, software and databases or micro-film or computer generated micro-fiche.

Information Assets : Means all information resources utilised in the course of any organisation's business and includes all information, application software (developed or purchased), and technology (hardware, system software and networks).

Information Technology Security : All aspects related to defining,

achieving and maintaining confidentiality, integrity, availability, accountability, authenticity and reliability.

Information Technology Security Policy : Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organisation and its Information Technology systems.

Information Warfare : Information Warfare is the competition between offensive and defensive players over information resources.

Input Validation Attacks : Input Validation Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

Integrity : Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Integrity Star Property : In Integrity Star Property a user cannot read data of a lower integrity level then their own.

Intermediary : With respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

Internet : A term to describe connecting multiple separate networks together.

Internet Control Message Protocol (ICMP) : An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Engineering Task Force (IETF) : The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Architecture Boards (IAB). IETF members are drawn from the Internet Society's individual and organisation membership.

Internet Message Access Protocol (IMAP) : A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for an extension to the Post Office Protocol (POP). It is defined in RFC 1203 (v3) and RFC 2060 (v4).

Internet Protocol (IP) : The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec) : A developing standard for security at the network or packet processing layer of network communiation.

Internet Service Providers (ISP) : A company that provides access to the internet.

Internet Standard : A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with sustantial operational experience, enjoys significant public support, and is recognisably useful in some or all parts of the Internet.

Interanet : A computer network, especially one based on Internet technology, that an organisation uses for its own internal, and usually private, purposes and that is closed to outsiders.

Instant Messanger : It is a kind of communication service available on internet that enables a user to create a private room with another person.

Intrusion Detection : A security management system for computers and networks. An IDS gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusion (attacks from outside the organisation) and misuse (attacks from within the organisation).

IP Address : A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Flood : A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP Forwarding : IP forwarding is an operating system option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Spoofing : The techniques of supplying a false IP address.

ISO : International Organisation for Standardisation, a voluntary, non-treaty, non-government organisation, established in 1947, with voting members that are designated standard bodies of participating nations and non-voting observer organisations.

Issue-Specific Policy : An Issue-Specific Policy is intended to address specific needs within an organisation such as password policy.

ITU-T : International Telecommunications Union, Telecommunication Standardisation Sector (formerly "CCITT"), a United Nations treaty organisation that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations".

J

Jitter : Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.

Jump Bag : A Jump Bag is a container that has all the items necessary to respond to an incident inside to help mitigate the effects of delayed reactions.

K

Keyberos : A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service-distributed in a client-server network environment.

Kernel : The essential centre of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

Key : A sequence of symbols that controls the operation of a cryptographic transformation (e.g., encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

Key Generation : The trustworthy process of creating a private key/public key pair.

Key Management : The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Key Pair : In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

L

Lattice Techniques : Lattice Techniques use security designations to determine access to information.

Layer 2 Forwarding Protocol (L2F) : An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP) : An extension of the Point-to-Point Tunneling used by an Internet service provider to enable the operation of a virtual private network over the Internet.

Least Privilege : Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legion : Software to detect unprotected shares.

Licence : Means a licence granted to a Certifying Authority.

Lightweight Directory Access Protocol (LDAP) : A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Link State : With link state, routes, maintain information about all routers and router-to-router links within a geographic area, and creates a table of best routes with that information.

List Based Access Control : List Based Access Control associates a list of users and their privileges with each object.

Loadable Kernel Modules (LKM) : Loadable Kernel Module

allow for the adding of additional functionality directly into the kernel while the system is running.

Local Area Network (LAN) : It is kind of network used for connecting two or more computer situated at close distance, i.e., building, office, etc.

Log Clipping : Log clipping is the selective removal of log entries from a system log to hide a compromise.

Logic Bomb : It is an innocent looking program used by a hacker to collect data like passwords, credit card number, etc.

Logic Gate : A logic gate is an elmentary building block of a digital circuit. Most logic gates have two inputs and one output. As ditial circuit can only understand binary inputs and outputs can assume only one of two states, 0 or 1.

Loopback Address : The loopback address (127.0.0.1) is a pseudo IP address that always refer back to the local host and are never sent out onto a network.

Love Bug : A form of Virus.

Low Sensitive : Applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure.

M

MAC Address : A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

Macomb Area Computer Software Team (MACE) : A task force of law enforcers of U.S.A. dealing with computer related crimes.

Malicious Code : Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorised access to system resources or tricks a user into executing other malicious logic.

Malicious Programs : It is computer programs, such as virus, Trojan, logic bomb, etc., intended to cause harm to computer network.

Malware : A generic term for a number of different types of malicious code.

Manadatory Access Control (MAC) : Manadatory Access Control

controls is where the system control access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

Management of Digital Signature Certificate : (*See* Certificate Management).

Masquerade Attack : A type of attack in which one system entity illegitimately poses as (assumed the identity of) another entity.

Measures of Effectiveness (MOE) : Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

Media : The material or configuration on which data is recorded. Examples include magnetic taps and disks.

Message : A digital representation of information; a computer-based record. A subject of record. (*See* also record).

Mobile Cloning : It is a criminal act, where security data of a mobile is reprogrammed into another mobile, so that calls could be made from both phone but billing with from original phone only.

Monoculture : Monoculture is the case where a large number of users run the same software, and are vulnerable to the same attacks.

Morris Worm : A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November 1988, causing problems for thousands of hosts.

Multi-Cast : Broadcasting from one host to a given set of hosts.

Multi-Homed : You are "multi-homed" if your network is directly connected to two or more ISP's.

Multiplexing : To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

N

Name : A set of identifying attributes purported to describe an entity of a certain type.

National Institute of Standards and Technology (NIST) : National Institute of Standards and Technology, a unit of the US Commerce

Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Disaster : Any 'act of God' (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Netmask : 32-bit number indicating the range of IP addresses residing on a single IP networks/subnet/supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.

Network : A set of related, remotely connected devices and communications facilities including more than one computer system with the capacity to transmit data among them through the communications facilities.

Networking : An act of establishing interconnection among more than one computer for enabling them to exchange data between them.

Network Administrator : The person at a computer network installation who designs, controls, and manages the use of computer network.

Network Address Translation : The translation of an Internet Protocol addressed used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

News Group : It is an online discussion group that may be accessed through internet.

Network-Based IDS : A network-based IDS monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match

a signature. Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

Network Mapping :To compile an electronic inventory of the systems and the services on your network.

Network Taps : Network taps are hardware devices that hook directly onto the network cable and send a copy of the traffic that passes through it to one or more other networked devices.

Node : In a network, a point at which one or more functional units connect channels or data circuits.

Nominated Website : A website designated by the Certifying Authority for display of information such as fee schedule, Certification Practice Statement, Certificate Policy, etc.

Non-Printable Character : A character that doesn't have a corresponding ASCII code. Examples would be the Linefeed, which is ASCII character code 10 decimal, the Carriage Return, which is 13 decimal, or the bell sound, which is decimal 7. On a PC, you can often add non-printable characters by holding down the Alt key, and typing in the decimal value (i.e., Alt-007 gets you a bell). There are other character encoding schemes, but ASCII is the most prevalent.

Non-Repudiation : Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

Notary : A natural person authorised by an executive governmental agency to perform notarial services such as taking acknowledgment, administering oaths or affirmations, witnessing or attesting signatures, and noting protests of negotiable instruments.

Null Session : Known as Anonymous Logon, it is a way of letting an anonymous user retrieve information such as user names and shares over the network or connect without authentication. It is used by applications such as explorer .exe to enumerate shares on remote servers.

O

Octet : A sequence of eight bits. An octet is an eight-bit byte.

One-Way Encryption : Irreversible transformation of plaintext to ciphertext, such that the plaintext cannot be recovered from the ciphertext by other than exhaustive procedures even if the cryptographic key is known.

One-Way Function : A (mathematical) function, f, which is easy to compute the output based on a given input. However, given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

On-Line : Communications that provide a real-time connection.

Open Shortest Path First (OSPF) : Open Shortest Path First is a link state routing algorithm used in interior gateway routing. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

Operations Zone : An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

Operational Certificate : A Digital Signature Certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

Operational Management : Refers to all business/service unit management (i.e., the user management) as well as Information Technology management.

Operational Period : The period starting with the date and time a Digital Signature Certificate is issued (or on a later date and time certain if stated in the Digital Signature Certificate) and ending with the date and time on which the Digital Signature Certificate expires or is earlier suspended or revoked.

Organisation : An entity with which a user is affiliated. An organisation may also be a user.

Originator : A person who sends, generates, stores or transmits any electronic message or causes any electronic message to be

sent, generated, stored or transmitted to any other person but does not include an intermediary.

OSI : OSI (Open System Interconenction) is a standard description or 'reference model' for how message should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

OSI layers : The main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. Each communicating user of program is at a computer equipped with these seven layers of function. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program. The actual programming and hardware that furnishes these seven layers of function is usually a combination of the computer operating system, applications (such as your Web browser), TCP/IP or alternative transport and network protocols, and the software and hardware that enable you to put a signal on one of the lines attached to your computer. OSI divides telecommunication into seven layers. The layers are in two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer or router. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed up to the upper layers but are forwarded to another host. The seven layers are : Layer 7 : The application layers... This is the layer at which communication

partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform layer functions.) Layer 6 : The presentation layer... This is a layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). Sometimes called the syntax layer. Layer 5 : The session layer... This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications to each end. It deals with session and connection coordination. Layer 4 : The transport layer... This layer manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer. Layer 3 : The network layer... This layer handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer does routing and forwarding. Layer 2 : The data-link layer... This layer provides synchronisation for the physical level and does bit-stuffing for strings of 1's in excess of 5. It furnishes transmission protocol knowledge and management. Layer 1 : The physical layer... This layer conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier.

Overload : Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

P

Packet : A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Switched Network : A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

Particularly Sensitive : Applies to information that, if compromised, could reasonably be expected to cause serious injury

outside the national interest, for example, loss of reputation or competitive advantage.

Partitions : Major divisions of the total physical hard disk space.

Password (Pass Phrase; Pin Number) : Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.

Password Authentication Protocol (PAP) : Password Authentication Protcol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

Password Cracking : Password cracking is the process of attempting to guess passwords, given the password file information.

Password Sniffing : Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

PC Card : (*See* also Smart Card) : A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

Patch : A patch is a small update released by a software manufactures to fix bugs in existing programs.

Patching : Patching is the process of updating software to a different version.

Payload : Payload is the actual application data a packet contains.

Penetration : Gaining unauthorised logical access to sensitive data by circumventing a system's protections.

Penetration Testing : Penetration testing is used to test the external perimeter security of network or facility.

Permutation : Permutation keeps the same letters but changes the position within a text to scramble the message.

Person : Means any company or association or individual or body of individuals, whether incorporated or not.

Personal Firewalls : Personal firewalls are those firewalls that are installed and run on individual PCs

Personal Presence : The act of appearing (physically rather than virtually or figuratively) before a Certifying Authority or its designee and providing one's identity as a prerequisite to Digital Signature Certificate issuance under certain circumstances.

Phreaking : It covers a wide variety of activities concerning the abuse of telephone network.

Ping of Death : An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Ping Scan : A ping scan looks for machines that are responding to ICMP Echo Requests.

Ping Sweep : An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

PKI (Public Key Infrastructure)/ PKI Server : A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital Signature Certificates and public-private key pairs, including the ability to generate, issue, maintain and revoke public key certificates.

PKI Hierarchy : A set of Certifying Authorities whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior Certifying Authority.

Plaintext : Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Pledge : (*See* Software Publisher's Pledge).

Policy : A brief document that states the high-level organisation position, states the scope, and establishes who is responsible for compliance with the policy and the corresponding standards. Following is an abbreviated example of what a policy may contain:

- Introduction
- Definitions
- Policy Statement identifying the need for 'something' (e.g., data security)
- Scope
- People playing a role and their responsibilities
- Statement of Enforcement, including responsibility.

Point-to-Point Protocol (PPP) : A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

Point-to-Point Tunneling Protocol (PPTP) : A protocol (set of communication rules) that allows corporations to extend their own corporate network through private 'trunnels' over the public Internet.

Poison Reverse : Split horizon with poisoned reverse (more simply, poison reverse) does include such routes in updates, but sets their metrics to infinity. In effect, advertising the fact that there routes are not reachable.

Polyinstantiation : Polyinstatiation is the ability of a database to maintain multiple records with the same key. It is used to prevent inference attacks.

Polymorphism : Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port : A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.

Port Scan : A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a 'well-known' port number, the computer provides. Port scanning, a favourite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Possession : Possession is the holding, control, and ability to use information.

Post Office Protocol, Version 3 (POP3) : An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

Practical Extraction and Reporting Language (Perl) : A script programming language that is similar in syntax to the C language

and that includes a number of popular Unix facilities such as sed, awk, and tr.

Preamble : A preamble is a signal used in network communications to synchronise the transmission timing between two or more systems. Proper timing ensures that all systems are interpreting the start of the information transfer correctly. A preamble defines a specific series of transmission pulses that is understood by communicating systems to mean "someone is about to transmit data". This ensures that systems receiving the information correctly interpret when the data transmission starts. The actual pulses used as a preamble vary depending on the network communication technology in use.

Pretty Good Privacy (PGP) TM : Trademark of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

Private Addressing : IANA has set aside three address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in RFC 1918. The reserved address blocks are : 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172/16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix).

Private Key : The key of a key pair used to create a digital signatures.

Procedure : A set of steps performed to ensure that a guideline is met.

Program : A detailed and explicit set of instructions for accomplishing some purpose, the set being expressed in some language suitable for input to a computer, or in machine language.

Program Infector : A program infector is a piece of malware that attaches itself to existing program files.

Program Policy : A program policy is a high-level policy that sets the overall tone of an organisation's security approach.

Promiscuous Mode : When a machine reads all packets off the network, regardless of who they are addressed to. This is used by network administrators to diagnose network problems, but also by unsavory characters who are trying to eavesdrop on network traffic (which might contain passwords or other information).

Proprietary Information : Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Protocol : A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a communication connection.

Protocol Stacks (OSI) : A set of network protocol layers that work together.

Proxy Server : A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Access Zone : Generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorised activity.

Public Key : The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Cryptography : A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Encryption : The popular synonym for 'asymmetric cryptography'.

Public Key Infrastructure (PKI) : A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to security and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a

digital certificate that can identify an individual or an organisation and directory services that can store and, when necessary, revoke the certificates.

Public Key Forward Secrecy (PFS) : For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

Q

QAZ : A network worm.

R

Race Condition : A race condition exploits the small windows of time between a security control being applied and when the service is used.

Radiation Monitoring : Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Recipient (of a Digital Signature) : A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs. (*See also* relying party)

Reconnaissance : Reconnaissance is the phase of an attack where an attacker finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.

Record : Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term 'record' is a superset of the two terms 'document' and 'message'. (*See also* document, message).

Re-enrolment : (*See also* Renewal)

Reflexive ACLs (Cisco) : Reflexive ACLs for Cisco routers are a step towards making the router act like a stateful firewall. The router will make filtering decisions based on whether connections are a part of established traffic or not.

Registry : The Registry in Windows operating systems is the central set of settings and information required to run the Windows computer.

Rely/Reliance (on a Certificate and Digital Signature) : To accept a digital signature and act in a manner that could be detrimental

to oneself were the digital signature to be ineffective. (See also relying party; receiption).

Relying Party : A recipient who acts in reliance on a certificate and digital signature. [*See also* recipient; rely or reliance (on a certificate and digital signature)].

Renewal : The process of obtaining a new Digital Signature Certificate of the same class and type for the same subject once an existing Digital Signature Certificate has expired.

Repository : A database of Digital Signature Certificates and other relevant information accessible on-line.

Repudiation : (*See* also Non-repudiation)—The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

Request for Comment (RFC) : A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Resource Exhaustion : Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

Response : A response is information sent that is responding to some stimulus.

Reverse Address Resolution Protocol (RARP) : RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control—MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Reverse Engineering : Acquiring sensitive data by disassembling and analysing the design of a system component.

Revoke a Certificate : The process of permanently ending the operational period of a Digital Signature Certificate from a specified time forward.

Reverse Lookup : Fill out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.

Reverse Proxy : Reverse proxies take public HTTP request and pass them to back-end webservers to send the content to it, so the proxy can then send the content to the end-user.

Risk : Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Analysis : The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

Risk Assessment : An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

Risk Management : The total process of identifying, controlling, and eliminating or minimising uncertain events based on estimated probabilities of the occurrence of those events.

Rivest-Shamir-Adleman (RSA) : An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Role Based Access Control : Role based access control assigns users to roles based on their organisational functions and determines authorisation based on those roles.

Root : Root it the name of the administrator account in Unix systems.

Rootkit : A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator level access to a computer or computer network.

Router : Router interconnect logical networks by forwarding information to other networks based upon IP addresses.

Routing Information Protocol (RIP) : Routing Information Protocol is a distance-vector protocol used for interior gateway routing which uses hop count as the sole metric of a path's cost.

Routing Loop : A routing loop is where two or more poorly configured routers repeatedly exchange the same packet over and over.

RPC Scans : RPC scans determine which RPC services are running on a machine.

Rule Set Based Access Control (RSBAC) : Rule Set Based Access Control targets actions based on rules for entities operating on objects.

S

S/Key : A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user logic. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Search Engine : It is an enquiry programme that searches documents or information against specific key words and returns a list of the documents.

Safety : Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors are protected from harm.

Scavenging : Searching through data residue in a system to gain unauthorised knowledge of sensitive data.

Secret Share : A portion of a cryptographic secret split among a number of physical tokens.

Secret Share Holder : An authorised holder of a physical token containing a secret share.

Secure Channel : A cryptographially enhanced communications path that protects messages against perceived security threats.

Secure System : Means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures.

Secure Electronic Transactions (SET) : Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SH) : A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL) : A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection

Security : The quality or state of being protected from unauthorised access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific 'state' to be preserved under various operations.

Security Policy : A set of rules and practices that specify or regulate how a system or organisation provides security services to protect sensitive and critical system resources.

Security Procedure : Means the security procedure prescribed under section 16 of the Information Technology Act, 2000.

Security Services : Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity.

Security Zone : An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 weeks by security staff, other personnel or electronic means.

Segment : Segment is another name for TCP packets.

Self-Signed Public Key : A data structure that is constructed the same as a Digital Signature Certificate but that is signed by its subject. Unlike a Digital Signature Certificate, a self-signed public key cannot be used in a trustworthy manner to authenticate a public key to other parties.

Sensitive Information : Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties : Separation of duties is the principle of splitting privileges among multiple individuals or systems.

Serial Number : (*See* certificate serial number)

Server : A system entity that provides a service in response to requests from other system entities called clients.

Session : A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking : Take over a session that someone else has established.

Session Key : In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

Shadow Password Files : A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

Share : A share is a resource made public on a machine, such as a directory (file share) or printer (printer share).

Shell : A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

Sign : To create a digital signature for a message, or to affix a signature to a document, depending upon the context.

Signals Analysis : Gaining indirect knowledge of communicated data by monitoring and analysing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Signature : Signature is a distinct pattern in network traffic that can be identified to a specific tool exploit.

Signer : A person who creates a digital signature for a message, or a signature for a document.

Simple Integrity Property : Simple Integrity Property a user cannot write data to a higher integrity level than their own.

Simple Network Management Protocol (SNMP) : The protocol governing network management and the monitoring of network devices and their functions. A set of protocols for managing complex networks.

Simple Security Property : Simple Security Property a user cannot read data of a higher classification than their own.

Smart Card : A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/Mime : A specification for E-mail security exploiting a cryptographic message syntax in an Internet mime environment.

Smurf : The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer : A sniffer is a tool that monitors network traffic as it is received in a network interface.

Sniffing : A synonym for "passive wiretapping".

Social Engineering : A euphemism for non-technical or low-technology means—such as lies, impresonation, tricks, bribes, blackmail and threats—used to attack information systems.

Socket : The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

Socket Pair: A way to uniquely specify a connection, i.e.,

source IP address, source port, destination IP address, destination port.

Socks : A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. SOCKS uses sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software : Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Software Piracy : An act of making duplicate or ingenuine software copying from original copy.

Source Port : The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

Spamming : Sending of bulk and unrepeated unsolicited e-mails.

Spam : Electronic junk mail or junk newsgroup postings.

Spanning Port : Configures the switch to behave like a hub for a specific port.

Split Key : A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

Split Horizon : Split horizon is a algorithm for avoiding problems caused by including routes in updates sent to the gateway from which they were learned.

Spoof : Attempt by an unauthorised entity to gain access to a system by posing as an authorised user.

SQL Injection : SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

Stack Mashing : Stack mashing is the technique of using a buffer overflow to trick a computer into executing arbitrary code.

Standard ACLs (Cisco) : Standard ACLs on Cisco routers make packet filtering decisions based on Source IP address only.

Star Property : In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

State Machine : A system that moves through a series of progressive conditions.

Stateful Inspection : Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Static Host Tables : Static host tables are text files that contain hostname and address mapping.

Static Routing : Static routing means that routing table entries contain information that does not change.

Stealthing : Stealthing is a term that refers to approaches used by malicious code to conceal its presence of the infected system.

Steganalysis : Steganalysis is the process of detecting and defeating the use of steganography.

Steganography : Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is "invisible" ink.

Stimulus : Stimulus is network that initiates a connection or solicits a response.

Store-and-Forward : Store-and-Forward is a method of switching where the entire packet is read by a switch to determine if it is intact before forwarding it.

Straight-Through Cable : A straight-through cable is where the pins on one side of the connector are wired to the same pins on the other end. It is used for interconnection nodes on the network.

Stream Cipher : A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

Strong Star Property : In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

Subject (of a Certificate) : The holder of a private key corresponding to a public key. The term 'subject' can refer to both the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject's Digital Signature Certificate.

Subject Name : The unambiguous value in the subject name field of a Digital Signature Certificate, which is bound to the public key.

Subscriber : A person in whose name the Digital Signature Certificate is issued.

Subscriber Agreement : The agreement executed between a subscriber and a Certifying Authority for the provision of designated public certificate services in accordance with this Certification Practice Statement.

Subscriber Information : Information supplied to a certification authority as a part of a Digital Signature Certificate application. (*See* also certificate application).

Sub Network : A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

Subnet Mask : A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

Suspend a Certificate : A temporary 'hold' placed on the effectiveness of the operational period of a Digital Signature Certificate without permanently revoking the Digital Signature Certificate. Digital Signature Certificate suspension is invoked by, e.g., a CRL entry with a reason code. (See also revoke a certificate).

Switch : A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

Switched Network : A communications network, such as the public switched telephone network, in which any user may be connected to any other through the use of message, circuit, or packet switching and control devices.

Symbolic Links : Special files which point at another file.

Symmetric Cryptography : A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such s encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

Symmetric Key : A cryptographic key that is used in a symmetric cryptographic algorithm.

SYN Flood : A denial of service attack that sends a host more TCP SYN packets (request to synchronise sequence numbers, used when opening a connection) than the protocol implementation can handle.

Synchronization : Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

Syslog : Syslog is the system logging for Unix systems.

System Administrator : The person at a computer installation who designs, controls, and manages the use of the computer system.

System Security : A system function that restricts the use of objects to certain users.

System Security Officer (SSO) : A person responsible for enforcement or administration of the security policy that applies to the system.

System Software : Application-independent software that supports the running of application software. It is a software that is part of or made available with a computer system and the determines how application programs are run; for example, an operating system.

System-Specific Policy : A system-specific policy is a policy written for a specific system or device.

T

T1, T3 : A digital circuit using TDM (Time Division Multiplexing).

Tamper : To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorised functions or services.

TCP Fingerprinting : TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

TCP Full Open Scan : TCP Full Open Scans check each port by performing a full three-way handshake on each port to determine if it was open.

TCP Half Open Scan : TCP Half Open Scans work by performing the first half of three-way handshake to determine if a port is open.

TCP Wrapper : A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

TCP/IP : A synonym for "Internet Protocol Suite", in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

TCPDump : TCPDump is a freeware protocol analyser for Unix that can monitor network traffic on a wire.

Technology Convergence : It is convergence of two or more disparate disciplines or technologies i.e. Fax, which is convergence of telecommunication and printing technology.

Telecommunication Theft : A criminal act where a hacker invades into communication network to make their own fake calls.

Telnet : A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

Test Certificate : A Digital Signature Certificate issued by a Certifying Authority for the limited purpose of internal technical testing. Test certificates may be used by authorised persons only.

Threat : A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment : A threat assessment is the identification of types of threats that an organisation might be exposed to.

Threat Model : A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector : The method a threat uses to get to the target.

Time-out : A security feature that logs off a user if any entry is not made at the terminal within a specified period of time.

Time Stamp : A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

Time to Live : A value in an Internet Protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

Tiny Fragment Attack : With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter. STD 5, RFC 791 states : Every Internet module must be able to forward a datagram of 68 octets without further fragmentation. This is because an Internet header may be up to 60 octets, and the minimum fragment is 8 octets.

Token : A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificate, including all certificates in the user's certification chain.

Token-Based Access Control : Token-based access control associates a list of objects and their privileges with each user. (The opposite of list based).

Token-Based Devices : A token-based device is triggered by the time of day, so every minute the password changes, requiring the user to have the token with them when they log in.

Token Ring : A token ring network is a local area network in

which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

Topology : The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. The specific physical, i.e., real, or logical, i.e., virtual, arrangement of the elements of a network. Note 1 : Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Note 2: The common types of network topology are illustrated.

Traceroute (taxcert.exe) : Traceroute is a tool that maps the route a packet takes from the local machine to a remote destination.

Transmission Control Protocol (TCP) : A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transaction : A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

Transport Layer Security (TLS) : A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

Triple DES : A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effectively key length of 112 or 168 bits.

Triple-Wrapped : S/NIME usage : data that has been signed

with a digital signature, and then encrypted, and then signed again.

Trojan Horse : A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program.

Trunking : Trunking is connecting switched together so that they can share VLAN information between them.

Trust : Trust determines which permissions and what actions other systems or users can perform on remote machines.

Trusted Ports : Trusted ports are ports below number 1024 usually allowed to be opened by the root user.

Trusted Position : A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital Signature Certificates, including operations that restrict access to a repository.

Trusted Third Party : In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (*Cf.*, trust)

Trustworthy System : Computer hardware, software, and procedures that are reasonably secure from intrustion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a 'trusted system' as recognised in classified government nomenclautre.

Tunnel : A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link—i.e., as OSI layer 2 connection—created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunneling can move data between computers that use a protocol not supported by the network connecting them.

Type (of Certificate) : The defining properties of a Digital Signature Certificate, which limit its intended purpose to a class of applications uniquely, associated with that type.

U

UPD Scan : UDP scans perform scans to determine which UDP ports are open.

Unicast : Broadcasting from host to host.

Uniform Resource Identifier (URI) : The generic term for all types of names and addresses that refer to objects on the World Wide Web.

Uniform Resource Locator (URL) : The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, http://www.pcwebopedia.com/index.html

Unix : A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programmers, Unix was designed to be a small, flexible system used exclusively by programmers.

Unprotected Share : In Windows terminology, a "share" is a mechanism that allows a user to connect to file systems and printers on other systems. An "unprotected share" is one that allows anyone to connect to it.

User : A person, organisation entity, or automated process that accesses a system, whether authorised to do so or not.

User Contingency Plan : User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

V

Valid Certificate : A Digital Signature Certificate issued by a Certifying Authority and accepted by the subscriber listed in it.

Validate a Certificate : The process performed by a recipient or relying party to confirm that an end-user subscriber Digital Signature Certificate is valid and was operational at the date and time a pertinent digital signature was created.

Validation (of Certificate Application) : The process performed by the Certifying Authority or its agent following submission of a Digital Signature Certificate application as a prerequisite to approval of the application and the issuance of a Digital Signature Certificate. (*See also* authentication; software validation)

Validation (of Software) : (*See* Software Validation)

Verify (a Digital Signature) : In relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether :

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Virtual Private Network (VPN) : A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Virus : A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Vouyerism : An act done by a sexual pervert who derives gratification from surreptitiously watching sexual acts or objects *with web camera, etc.*

Vulnerability : A flaw or weakness in a system's design,

implementation, or operation and management that could be exploited to violate the system's security policy.

W

War Chalking : War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

War Dialer : A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing : War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

War Driving : War driving is the process of travelling around looking for wireless access point signals that can be used to get network access.

Web Portal : It is a service or a website that offers a broad array of resources and services.

Website : An individual network within the Internet.

Web Spoofing : An optical illusion where hyperlinks on web page can maintain character which look like real.

Web of Trust : A web of trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

Web Server : A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

Whois : An IP for finding information about resources on networks.

Wide Area Network (WAN) : It is a computer network based on geographically dispersed telecomunications.

Windowing : A windowing system is a system for sharing a computer's graphical display presentation resources among multiple applications at the same time. In a computer that has a graphical user interface (GUI), you may want to use a number of applications at the same time (this is called task). Using a separate

window for each application, you can interact with each application and go from one application to another without having to reinitiate it. Having different information or activities in multiple windows may also make it easier for you to do your work. A windowing system uses a window manager to keep track of where each window is located on the display screen and its size and status. A windowing system doesn't just manage the windows but also other forms of graphical user interface entities.

Windump : Windump is a freeware tool for Windows that is a protocol analyser that can monitor network traffic on a wire.

Wired Equivalent Privacy (WEP) : A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

Wireless Application Protocol : A specification for a set of communication protocols to standardise the way that wireless devices, such as cellular telephones and radio transcievers, can be used for Internet access, including e-mail, the World Wide Web, newsgroup, and Internet Relay Chat.

Wiretapping : Monitoring and recording data that is flowing between two points in a communication system.

World Wide Web ("the Web", WWW, W3) : The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

Worm : A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Wrap : To use cryptography to provide data confidentiality service for a data object.

Writing : Information in a record that is accessible and usable for subsequent reference.

X

XOR : An exclusive XOR operator used for logical operations.

X.509 : The ITU-T (International Telecommunications Union-T) standard for Digital Signature Certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

Y

Yankee-Doodle · It is name of a virus.

Z

Zone Transfer : A zone transfer is when a DNS server performs a complete dump of the database for a domain and sends the information from the primary DNS server to the secondary DNS servers.

Bibliography

I. Books

Hughes, A. Gordon, *Computer Contracts, Principles and Precedents.* Sweet and Maxwell, U.K.

Agrawal, H.O. (Dr.), *Human Rights,* Central Law Publication, Allahabad, 2004.

Anand, V.K. (Dr.), *Human Rights,* Allahabad Law Agency, Faridabad, 2001.

Metwell, A.W., and M. Manning, *Criminal Law,* Second Edition, 1985.

Ashworth, Andrew, *Principles of Criminal Law,* Clarendon Press, 1991.

Chandrasekhar Pillani, K.N., *General Principles of Criminal Law,* Eastern Book Company, Lucknow, 2003.

Chissek, Michael, *Electronic Commerce : Law and Practice,* Third Edition, Sweet and Maxwell Publication, London, 2002.

Cross, R. and Jones, P.A., *Introduction to Criminal Law,* Eighth Edition, London, 1976.

Mittal, D.P., *Law of Information Technology* (Cyber Law), Taxmann Allied Service Pvt. Ltd. Publishers, Delhi, 2000.

Lyoans, David, *Ethics and Rule of Law,* Cambridge University Press, London, 1984.

Rowland, Diana, *Information Technology Law,* 2nd Edition, Cavendish Publishing Limited, London, 2000.

Joga Rao, S.V., *Current Issues in Criminal Justice and Medical Law : A Critical Focus,* Eastern Law House, Kolkata, 1999.

Joga Rao, S.V., *Law of Cyber Crimes and Information Technology,* Wadhwa and Company, Nagpur, 2004.

Williams, G., *Text Book of Criminal Law,* Second Edition, Stevens, London, 1983.

Kapoor, Gopika Vaidya, *Cyber Crime Scene in India,* file : //cyber % crime % 20 scene % 20 in.

Fletcher, George, P., *Basic concepts of Criminal Law,* First Edition, Oxford University Press, 1998.

Smith, J.C., and Barian Hogan, *Criminal Law : Cases and Materials,* Fifth Edition, Butterworth, London, 1993.

Finnir, J.M., *Natural Law and Natural Rights,* Clarendon Press, Oxford, 1980.

Rosemary, J., and A. Hamilton, *Data Protection Law and Practice,* Sweet and Maxwell, London, 1999.

Feinberg, Joe, The Moral Limits of Criminal Law, Oxford University Press, 1994.

Kathuria, R.P., *Law of Crimes and Criminology,* Vinod Publications, Delhi, 2000.

Vijayshankar, N., *Cyber Laws for Every Netizen in India,* Ist Edition, Ujvala Consultants Pvt. Limited, Bangalore, 1999.

Kamath, Nandan, *Laws Relating to Computer, Internet and E-commerce,* Universal Law Publishing Co. Pvt. Limited, Delhi, 2000.

Nimmer, Raymond T., *The Law of Computer Technology : Rights, Licenses, Liabilities,* Warren Gorham Lamont, Boston, 1992.

Trilokekar, N.P., *A Practical Guide to IT Act, 2000;* Snowwhite Publications Pvt. Ltd., Mumbai, 2000.

Nugent, State Computer Statu, National Institute of Justice, U.S. Department of Justice, 1991.

Lawrence, Penelope, *Law on the Internet : A Practical Guide,* First Edition, Sweet and Maxwell, London, 2000.

Balasubramanyam, V., *Essays on the Penal Code,* Indian Law Institute, New Delhi, 1968.

Rosenoer, Jonathan, *Cyber Law : The Law of Internet*, Springer, New York, 1997.

Saxby, Stephen (ed.), *Encyclopaedia of Information Technology Law*, Sweet and Maxwell Publications, London, 2001.

Singh, P.K. (Dr.), *Supreme Court on Human Rights and Social Justice*, Allahabad Law Agency, Faridabad, 2001.

Dudeja, V.D., *Cyber Crimes and Law*, Commonwealth Publishers, Delhi, 2002.

Unni, V.K., *Trademark and Emerging Concepts of Cyber Property Rights*, Eastern Law House Pvt. Ltd., Kolkata, 2002.

Wall, David S., *Cyber Crimes : New Wine, no Bottles ? Invisible Crimes : Their Victims and their Regulation;* (edited) MacMillan, London, 1993.

II. Articles/ Research Papers

Admin, Computer Hacking : Where did it Begin and How did it Grow ? http://secinf.net/harmless_hacking_book/computer_hacking_where_did_it_begin_did_it_grow_html_Oct. 16, 2002.

Alexander Baranov, Digital Legislation, http://www.crimesearch.org/eng/library/Bara_nov_html.

Jerrett, Andrew and Iain Monaghan, The Internet : An Introduction for Lawyers, www.law.edu.ac. UK/Script/newscript/terrett.htm.

Belousov, Andrew, Some Aspects of Investigating Computer Crimes, www.crime_research.org/eng/library/Belousov0603_html.

Leiner, Barry M., *et.al.*, A Brief History of Internet, www.isoc.org/internet/history/briefs.html.

Givens, Beth, Identity Theft : How it Happens, Its Impact on Victims, and Legilsative Solution.

Harvey, Brian, What is a Hacker ? University of California, Berkley, http: //cs.berkeley.edu/bh/hacker.

Connel, Bruce Me, Sovereignty in Cyber Space, www.few.com/few/article/2000.

Code of Conduct for the Use of Software or Datasets, www.chest.ac.uk/conduct.html.

Combating Use of Internet to Exploit Children, www.iap.nl.com/exploit.html.

Computer Forensic Booms as Importance of Electronic Evidence Grows, Thomas Rude, Evidence Seizure Methodology for Computer Forensics, CISSP:http://www.crazytrain.com.seizure.html.

Cyber Crime Investigation and Prosecution, The Role of Penal and Procedural Law, E Law, *Murdoch University Electronic Journal of Law,* Vol. 8, No. 2, June, 2001, www.murdoch.edu.au/claw/claw/issues/v8n2/brenner 82 nf. html.

Cyber Law and Jurisdiction, www.geocities.com/jjwalsh1/cyber law.html.

Burk, Dan L., Jurisdiction in a World without Borders, *Virginia Journal of Law and Technology,* University of Virginia, Spring, 1997, www.gahtan.com/cgi_local/cyber law/jump.cgi? ID 675.

Carter, David L., and andra J. Katz, Computer Crime : An Emerging Challenge for Law Enforcement, http : //www.sgrm.com/art II.htm.

Loundy, David, Task Force Develops Privacy Principles, www.loundy.com/CDLB/IITF Privacy.html.

Debates Online Privacy Issues, www.wired.com/news/politics/01283, 13223, 00.html.

Declaration of Human Rights in Cyber Space, Draft Proposal, http.//www.be_in.com/10/rights dec.html.

Developments in Law, The Law of Cyber Space, http : //www.harvardlawreview.org/issues/112/7-1577.html.

Denning, Dorothy E., Cyber Terrorism, www.cosc.georgetown.edu/denning/infosec/cyberterror.html.

Thomas, Duglas, Analysis of a Hack, www.ojr.org/ojr/law/P1017967609.php.2002.

McGrath, Amy, Computer Hacking can Compromise Political Process, 26 Sept., 2001, www.hschapman.org.au/computer_hacking htm.

Mendes, E.P. , Human Rights and the New Information Technologies, The Law and Justice of Proportionality and Consensual Alliances.

F.B.I. Pursuing More Cyber Crime Cases, www.washinton_post.com.

Singh, Gurjeet and Vick Sandhu, Emergence of Cyber Crimes : A Challenge for the New Millenium, 2005 (1), *Crimes*, p. 484.

Human Rights online, http. //www.hro.org.

IT Laws in Australia, www_staff.mcs.uts.edu. au/-jim/cit2/site/law/Lawa Au Main Frame.htm.

Stanley, Janet, Child Abuse and the Internet, www.aifs.org.au/nch/issues/issues 15.html.

Taylor, Max, Ethel Quayle and G. Holland, Child Pornography, the Internet and Offending, www.isuma.net/vo2no2/taylor/taylor_e-shtml.

Naavi, Jurisdiction—A Nighmare for E-Business, February 7, 2003, www.naavi.org.

Chugh, Pooja, "DNA Technology and its Significance in the Detection of Crime in Modern Society's Crimes", 2005 (1) *Crimes*, p. 538.

Prosecuting Crimes Facilitated by Computers and by the Internet, www. cybercrime.gov/crimes.html.

Raghavan, R.K., Crimes in Cyber Space, www. front lineonnet.com /fl 1924/stories/ 20021206005111000.html.

Bortner, R. Mark, Cyberlaundering, Anonymous Digital Cash and Money Laundering, www. law.miami.edu/ froomkin/seminar/papers/brother.htm.

Standler, Ronald B., Computer Crime, http : //www.rbs2.com/ccrime.htm.

Hardman, Scott, Stalking : Impact, Law, Sentencing and Stalking on line, www. forensic_crim.com/readings/stalking.html.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July, 2002, www. cybercrime gov/s and smannual 2002.htm.

Search and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigatin, http : //www.cybercrime.gov/s and smanual 2002.htm.

Bharti, Smiti, Cyber Crime, A Define Challenge, File : // H:/ Articles % 20%-20% cyber % 20 crime.htm.

Software Piracy, www.sharemcoolnald.com/topic_0300.html.

Sehreider, Tari, Tracking down Cyber Criminal, Cyber Investigation, www.scmagazine.com.

The Good and Bad of Computer Hacking Source, www.isonline.com/bym/career/dec 02/101856.asp.

The Hacker's Code of Ethics, http : //Courses.cs.vt.edu/Professionalism/Worldcodes/Hackers.code.html.

The History of Hacking, www.roadnews.com/html/Articles/history of hacking.htm.

Lee, Tim Berners, The World Wide Web : Past, Present and Future, http : // www.w3.org/People/Berners_Lee/1996/ppf.html.

Wright, T.E., An Introduction to the Field Guide for Investigating Computer Crime, www.securityfocus.com/infocus/1244.

U.S. Government Forms Cyber Security Unit, www.asianlaws.org.

Polivanjuk, V., Crimes' Criminalistic Characteristic, The Electronic Frontier, The Challenge of Unlawful Conduct Involving the Use of the Internet, http : /www.cybercrime.gov.

Goluber, Viadimir, Cyber Terrorism as the New Form of Terrorism, www.crime-research.org.

Golubev, Vladmir, Tactical Feature of Inquiry Actions at Computer Crime Investigation, www.crime-research-org./eng/library/Golubev_may.html.

Jonathan, Wallace, and Mangan Mark, Sex, Laws, and Cyber Space, New York Holt, 1996, www.spectacle.org/freespen/contents.html.

Petherick, Wayne, Cyber Stalking : Obsessional Pursuit and The Digital Criminal, www. Crime library.com/criminology/cyber stalking/.

III. News Items/ Features

"Cyber Frontiers and the Path of Law", T.K. Vishwanathan, *The Hindu*, July 4, 2000.

"Sex and the Cellphone Camera", Submimal Bhattacharya, *Indian Express*, December 20, 2004.

"Great Indian Sexcapada", G.J.V. Prasad, *Indian Express*, December 28, 2004.

"Feminism in the Time of MMS, Amrita Sah, *The Indian Express*, January 4, 2005.

"E-mail Threat Highlight Need for Training in Cyber Crime", *The Hindu*, November 6, 2001.

"The Thanedaar State : Avinash Bajaj as India's First Prisoner of E-conscience", Ashok Malik, *The Indian Express*, December 22, 2004.

"Baazee.com's run_in with the law", Manoj Mitta, *The Indian Express*, December 23, 2004.

"Sex and Sensibility", Pratap Bhanu Mehta, *The Indian Express*, December 29, 2004.

"Keeping a Watch on Cyber Space", Sandeep Dikshit, *The Hindu*, April 23, 2005.

"China Teens Get Help for Net Addiction", *The Times of India*, July 3, 2005.

"Mobile Porn is Here to Stay", *The Times of India*, July 14, 2005.

"Mexican Porn Star in Mallika MMS", *The Times of India*, July 21, 2005.

"A Bug in My Phone", Swati Despande, *The Times of India*, July 21, 2005.

"Pornography Ka Khatra", Jagdish Chaturvedi, *Hindustan*, April 3, 2005.

"Popular Computer Game for Kids is Hidden Sex Trip", Katan Tanna and Nikhil Hemrajini, *The Times of India*, July 21, 2005.

IV. Websites

http : //www.washingtonpost.com

www. computer/world.com

www. crime-research.org

www. digital century.com

www. digital-convergence.org

www. internetnews.com

www. internetjournal.com

www. intranets.com
www. isc.org
www. legislation.hmso.gov.UK/acts
www. searchingineguide.com
www. webopedia.com
www. yourdictionary.com
www. healthepic.com
www. legalserviceindia.com
www. 1millionpapers.com
www. sejudgements.com
www. indianexpress.com
www. issueinmedicalethics.org