Cyber Laws For Every Netizen in India

(Version 2004)

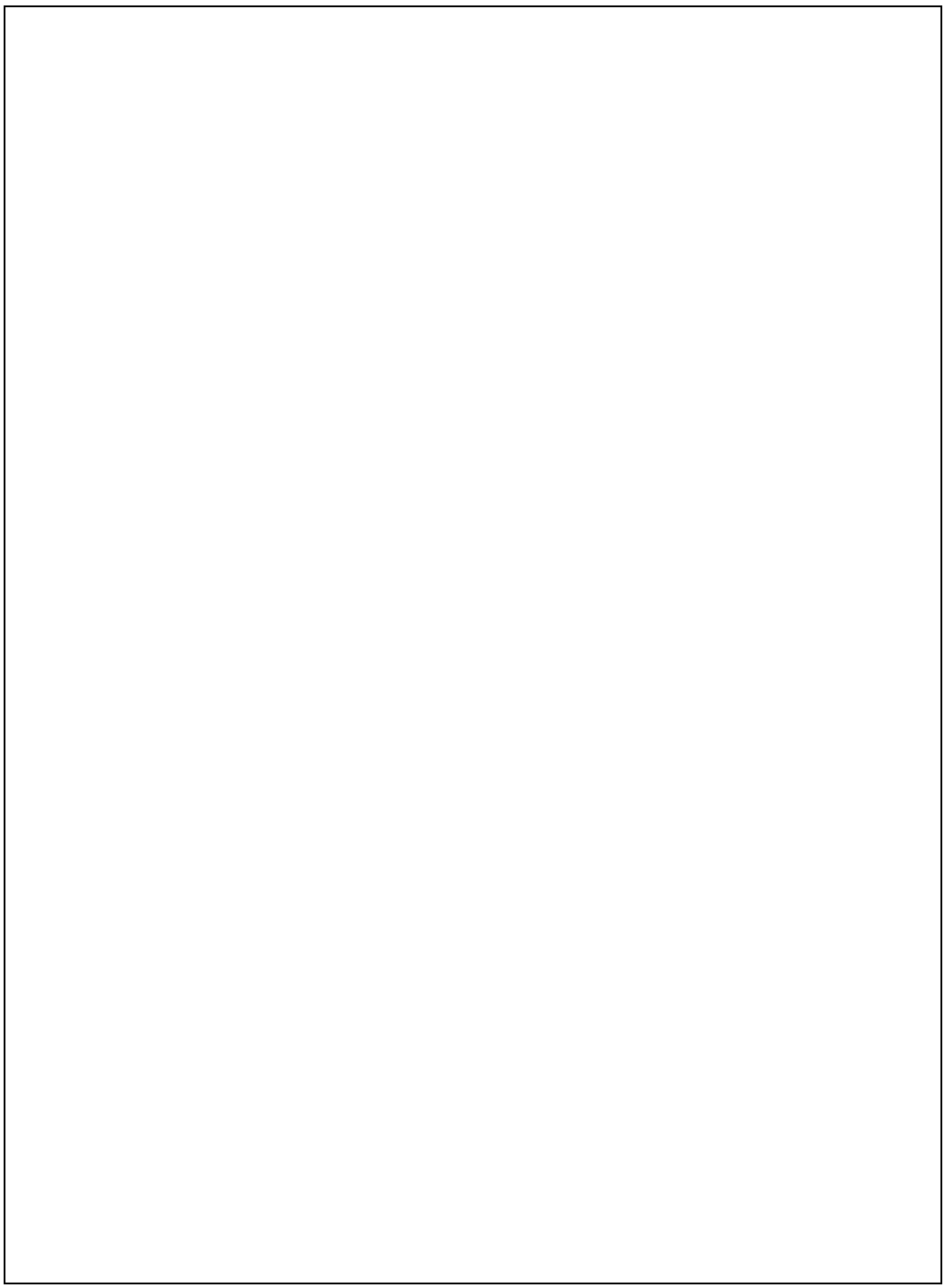
(With WSIS Declaration of Principles and Action Plan)

Naavi
Na.Vijayashankar
MSc.,CAIIB,CIIF,AIMADM
E-Business Consultant and Founder
www.naavi.org , www.cyberlawcollege.com

Published By

Ujvala Consultants Pvt Ltd
Admn Office: 11/10, R E Apartments,
Unnamalai Ammal Street, T.Nagar
Chennai-600017
E-Mail: ujvala@eth.net: Phone/Fax 044-28143448

January 2004



Cyber Laws For Every Netizen in India

(Version 2004)

(With WSIS Declaration of Principles and Action Plan)

Naavi
Na.Vijayashankar
MSc.,CAIIB,CIIF,AIMADM
E-Business Consultant and Founder
www.naavi.org , www.cyberlawcollege.com

Published By

Ujvala Consultants Pvt Ltd
Admn Office: 11/10, R E Apartments,
Unnamalai Ammal Street, T.Nagar
Chennai-600017
E-Mail: ujvala@eth.net: Phone/Fax 044-28143448

January 2004

Published by

Ujvala Consultants Pvt Ltd, 2003
Administrative Office:
11/10, R.E.Apartments
Unnamalai Ammal Street
T.Nagar
Chennai-600017
E-Mail: ujvala@eth.net

This work is based on the experience and views of the author which is to the best of his knowledge and belief correct and accurate at the time of writing. The opinion expressed herein will not however constitute legal advice and the author or the publisher is not responsible or liable for any actions of the readers based on the material contained in the book.

Index

Chapter	Title	Page
	Preface	**7**
Chapter I	Introduction	**13**
Chapter II	The Internet Era	**22**
Chapter III	Electronic Document	**37**
Chapter IV	Digital Signature	**52**
Chapter V	Digital Identity Management	**72**
Chapter VI	Business of Certifying Authorities	**89**
Chapter VII	Digital Contracts	**99**
Chapter VIII	Cyber Regulatory Structure	**112**
Chapter IX	Cyber Crimes	**121**
Chapter X	Intellectual Property Issues	**155**
Chapter XI	Network Service Providers	**186**
Chapter XII	Privacy and Personal Rights	**199**
Chapter XIII	Law Enforcement Issues	**240**
Chapter XIV	E Governance Issues	**249**
Chapter XV	Semi Conductor Act	**303**
Chapter XVI	Communication Convergence Bill	**308**
Chapter XVII	Business Opportunities in Cyber Law	**341**
Chapter XVIII	Legal Issues in Cyber Advertising	**349**
Chapter XIX	Legal Issues in Cyber Banking	**371**
Chapter XX	Legal Issues in Emerging Technologies	**393**
Chapter XXI	Legal Issues in Cyber Taxation	**406**
Chapter XXII	Cyber Wars and Cyber Terrorism	**416**
Chapter XXIII	Cyber Law Compliancy, The Need of the Hour	**431**
Chapter XXIV	Information System Security Audit	**442**
Chapter XXV	FAQ	**457**

PREFACE

Ever since a legal framework for the Cyber World was conceived in India, in the form of a draft E-Commerce Act 1998, the subject of Cyber Laws has fascinated me. Afterwards, the basic law for the Cyber space transactions in India has emerged in the form of the Information Technology Act 2000. It has further been supplemented with the Semi Conductor Integrated Circuits Layout Act. We are presently on the threshold of another major Cyber Regulation being passed in the form of the Communication Convergence Act.

The scope of Cyber Laws has therefore expanded more rapidly than what many considered possible in India given its huge rural population with low technology base.

The features of Cyber Law that attracts E-Business Professionals like me are ,

1. The close integration of technology in various aspects of law.
2. The dynamic nature of the evolving law and
3. The relative freshness of the Cyber Society where the fundamental principles of jurisprudence are yet to be developed.

These characteristics of Cyber Law are however also responsible for the discomfort those traditional legal professionals feel in studying this branch of law.

Firstly, the technology part of the law makes Cyber Law, a subject which cannot be understood without at least a small dose of technology input into the learning.

Secondly, the rapidly changing nature of the law is unnerving for the legal practitioner since the law seems to acquire new meaning with each succeeding new Act and each new judicial decision some where in the world.

Cyber Law has therefore emerged as a field of study for a new crop of professionals who may be called Techno-Legal specialists.

In India, the present educational system is such that a Technology student has no exposure to Law and a Law student has no exposure to Technology. Hence a Computer science student in a College is taught how to develop programs that can automatically transmit data across the Internet riding on a TCP/IP packet, without alerting him on cyber crimes such as Hacking or Virus introduction. The Law students on the other hand are taught about Trade Marks and Copyrights without recognizing their implications on the Electronic documents. As a result, neither the Technologist nor the Lawyer is trained in his formative years to understand Cyber Law.

I therefore felt that there was a need for techno-legal experts to de-mystify Cyber Law and make it possible for a large section of the society take up study of Cyber Law. It is envisaged that in future, Engineering, Commerce and Management Colleges will teach Cyber Law as an extension of Computer Science, Commerce and Management Education, even while the Law Colleges try to extend their coverage of Criminal Laws and IPR laws to the Cyber world.

The advent of Techno-Legal specialists will bring a change in the legal perspective in the country and we can expect that fresh ideas would emerge and form the building blocks for the development of Cyber Jurisprudence as a distinct field of study.

This book recognizes such a development and analyses different pieces of Cyber Legislation from a perspective that encourages debate rather than prescription.

The good reception received for my earlier book "Cyber Laws For Every Netizen in India" released in December 1999 which happened to be the first book on the subject of Cyber Laws to be published in India encouraged me to release the first E-Book on Cyber Laws entitled "Cyber Laws in India..ITA-2000 and Beyond" in May 2003. Since the release of the E-Book, there have been further changes in the Cyber Laws applicable to India.

This Book expands the content to the area of Cyber Security Audit with an exclusive chapter devoted to this subject which is of interest to the Chartered Accountants and Cyber Security professionals.

Yet another chapter that has been added is the Legal Issues in "Cyber Journalism" which focusses on the issues of Cyber Laws as applicable to Journalists.

As in the previous editions, the main objective of this book also is to serve the mission to spread Cyber Law Literacy. The goal is to reach as many of the professionals as possible not only in the Legal sector, but also in the Technology sector and Corporate Management sector.

Since, in future, "There is No Business Without E-Business", there will be no room for any corporate professional without a basic understanding of "Cyber Laws". Hence Cyber Law literacy amongst professionals such as Chartered Accountants, Company Secretaries, Bankers, Insurance professionals, Law Enforcement

officers, and E-Governance officials is as essential as the study of Company Law or Contract Law.

This book goes much beyond the Information Technology Act 2000 in discussing Cyber Laws as applicable in India. Cyber Squatting, Copyright Infringement and Patent Issues have been discussed in this book to the extent required.

Elements of Semi Conductor Integrated Circuit Layout Designs Act which is yet to be notified is also discussed considering it's importance.

A chapter has been devoted in the book on the Communication Convergence Act. Though the Communication Convergence Bill has presently been withdrawn from the Parliament, in view of the conceptual importance of this legislation and the possibility of its re-introduction with some modifications, the chapter has been retained.

The consequences of the recent amendments to the Negotiable Instruments Act 1881 through Negotiable Instruments Amendment Act 2002 have also been incorporated in appropriate places in the book.

Chapters on Privacy, E-Governance and Law Enforcement issues add up the comprehensiveness of this book.

Additionally there was a very significant Global development that took place in December 2003 which has transformed the future direction of the Cyber Society and the regulations that go with it. This refers to the World Summit on Information Society (WSIS) which was held in Geneva between December 10 to December 12, 2003. During this summit the representatives of all member

states of the United Nations Organizations have discussed the possible role of the sovereign Government states in the Information Society Management and adopted a " Declaration of Principles" and agreed to set up a working group to take the issue further for discussion in more concrete terms in the Tunisia summit in 2005. The historical imprint that this development creates cannot be lost sight of and a brief discussion on the same is included in this book.

The need to keep the book simple but yet cover a larger canvass has prompted me to add portions at the end of some of the chapters that stand out as independent articles. Some of them reflect the thoughts expressed by me in the website http://www.naavi.org in my humble opinion, add to the clarification of some of the points covered elsewhere in the book without disturbing the flow of discussions.

Maintaining the non legal style of the Book, as well as recognizing the evolving nature of the law, and also the lack of sufficient number of India specific cases, emphasis on Case Laws has been deliberately underplayed in the book. Some of the cases have however been referred to in the FAQ section.

I firmly believe that every judgment already delivered in Cyber Law cases is open to review and modification because of subsequent changes in technology and maturing of legal thoughts. Hence past judgments are treated more as stepping stones to understanding the nature of law rather than defining the legal precedence. I trust this change of emphasis is what makes this book more readable for corporate executives, e-commerce professionals and the common Netizens.

I would urge readers of this book to keep following the

developments in Cyber Law through the Cyber Law portal http://www.naavi.org so that they can follow the latest developments.

This version of the Book takes into consideration the fact that the book has been prescribed as a reference book in many of the Universities and Colleges for Management and other courses and contents prescribed as the syllabus for courses in Cyber Laws.

I hope the student community would find the Book useful for meeting their examination requirements also.

Naavi
December, 27, 2003

CHAPTER I

INTRODUCTION

RELEVANCE OF CYBER LAWS

If you are anybody other than a practicing Lawyer, the first question that would cross your mind when you start reading this book is whether the study of Cyber law is at all relevant for you.

The answer is a firm "yes". Cyber Law is a relevant knowledge for all of us living in a society with increasing use of Computers and you will appreciate this as you proceed to read more of this book.

The Cyber Laws that we are discussing here is the "Fundamental Law" of the Cyber Space. Whoever is living in this Cyber Space or is conducting business in Cyber Space or is exposed to Crimes in Cyber Space and Crimes emanating from Cyber Space, should all be concerned with this branch of Law.

In particular, Software professionals who actually create Cyber Space elements in the form of software products that communicate in Cyber Space and live for most part of their day in Cyber Space need to absorb many salient features of this Law so that they keep themselves and their clients safe and protected from the consequences of Cyber Law.

Corporate Executives who own and manage Cyber Space properties also need to be conversant with Cyber Laws so that they will be able to discharge their functions properly.

With the passage of the Information Technology Act 2000, (ITA-2000) with effect from October 17, 2000 India has decisively moved from a paper Based society to a paper less society.

As per the provisions of the ITA-2000, Records and Signatures in Electronic form will have complete legal effect, validity or enforceability in all transactions except for the following five types of transactions **specifically excluded** in the Act.

- Negotiable Instruments (Other than Cheques)
- Power of Attorney instruments,
- Trust deeds,
- Wills, and
- Any contract of sale or conveyance of immovable property or interest in such property.

In bringing Digital Documents and Signatures within the ambit of law, ITA-2000 has used a "Bridging Provision" to state that "Wherever Law" requires documents to be in writing and to be "Signed", the requirement will be deemed to have been satisfied if such a document is rendered in electronic form and the signature is rendered in the manner specified in the Act.

By virtue of this, every law in India today stands extended to Electronic Documents excepting the categories mentioned in the earlier paragraph.

ELECTRONIC AGREEMENTS ARE NOW LEGALLY VALID

Thus, with the passage of the Act, most of the contracts that we need in the commercial world can be created without the need to have written instruments. Any person may send you an "offer" through an electronic document and if you are prepared to respond by accepting the offer electronically, an agreement valid in law can be concluded.

Most of the international contracts have already moved into electronic form and all Exporters and Importers need to familiarize themselves with the provisions of the act to be able to respond to the needs of the international commercial world.

An ordinary Internet user while surfing a web site may be offered electronic documents to approve and he can instantly conclude contracts by clicking his acceptance.

It is also envisaged that many contracts could be partially concluded in the electronic form and partly in writing. This may mean that for some of your transactions in the real society, you may be forced to resort to electronic documents.

For example, you may buy a TV from a shop but its warranty may be administered through the web. If you like to invoke the warranty, one of the accepted modes could be through digitally signed electronic notices.

GOVERNMENT GOES ELECTRONIC

After Information Technology Act 2000, Government departments can issue permits, licenses etc in electronic form. They may also distribute and receive tender applications online. They can receive payments, retain documents and issue Gazettes in the electronic form.

Even though the ITA-2000 makes provisions for Government transactions to be done through electronic documents, keeping in view the need for a smooth transition from the Paper based Society to the Digital Society, the Act has stated that no right will be conferred on the Citizens to insist that any Government Department has to adopt Electronic means for either acceptance

of electronic applications, retention of documents in electronic form and accept electronic form of acceptance of money.

Many State Governments have taken aggressive measures to use E-Tendering, E-Applications and E-Payments for Government work. Common man therefore is already pushed into the use of E-Contracts in Government transactions also.

COMPUTER CRIMES ARE PUNISHABLE

Over and above the specific electronic contracts you may enter into, the enactment of Cyber laws recognizes certain actions as "Punishable Offences". It is necessary for every user of Internet and other proprietary networks to avoid committing any act, which can be termed as such "Computer Crime".

Some of the Crimes may result in a liability to compensate the affected person to the extent of Rs 1 crore and some may land the offender in jail up to 10 years. When the Communication Convergence Bill becomes an Act, the limit for compensation may even go up to Rs 50 crores.

IGNORANCE IS NO DEFENCE

As all transactions around us tend to involve computers and electronic documents, it becomes necessary for every individual whether or not he is an Internet user, to familiarize him with the proposed laws.

His legal liabilities in these cases get crystallized because he is part of a system where computers have become a device of common usage.

We know that ignorance of law is no defense in a legal suit. If citizens don't keep themselves informed about the technological developments that could affect their legal responsibilities, they may in consequence get penalized for their ignorance.

INTERNET IS A PART OF OUR ENVIRONMENT

The day has now arrived when Internet and Computer Network have become as much a part of our society as the Public Road, Gas or Electricity is. While some of us may personally not like to use this gadget at present, or use it only for restricted purposes, the environment may force encounters with the Cyber world and impinge on us liabilities that we never thought were ours.

CYBER LAWS ARE ALREADY HERE SINCE OCTOBER 17, 2000

With the passage of the Information Technology Act-2000, the legal system in India has moved towards adoption of Digital technology as a replacement to the Paper based systems.

The laws are now in force since October 17, 2000 and since more than three years have passed since the law became enforceable, any further delay in putting the law into practice would not be condoned by either the society or the judiciary.

As long as there were no Cyber Laws in force in the country, it was perhaps not damaging to click away for fun. Now, if we continue to click blindly while on the Net, we may pick up legal liabilities that could be crippling.

PROTECT YOURSELF BY BEING CYBER LITERATE

Knowledge of Cyber Laws are therefore essential for every person who may directly or indirectly interact with networked services either over the Internet or other proprietary networks of Banks, Stock Brokers, Intra-Company and Inter-Company information exchange systems.

You should therefore know what constitutes "Digital Signature", "What is a Digitally signed Electronic Document", "How Electronic Contracts can be completed", "What constitutes a Computer Crime" and such other aspects that may affect you as a Netizen in the Cyber World as well as a Citizen of India.

Digital Contract Era Dawns on India

(A Perspective View of India's Journey into the Digital Contract Era)

October 17, 2000 will be an important day in the e-history of India (and the General History of India as well). This was the day when India entered the "Digital Contract Era" with the notification of the Rules under the Information Technology Act 2000. With this, the story which began with the drafting of the E-Commerce Act 98 reached a decisive stage where Electronic Documents and Digital Signatures became as valid as paper documents and written signatures.

It was in December 1999 that the Information Technology Bill 99 was presented in the Parliament by the Honourable Minister of Information Technology Mr Pramod Mahajan. The Bill was referred to a select Parliament committee.

The outbreak of the "I Love You" virus galvanized the Bill and the standing committee presented an amended form of the Bill on May 14, 2000 to the Parliament for debate and passage.

After a quick round of discussions with NASSCOM, which resulted in the dropping of a few clauses on "Registration of Websites" and "Monitoring of Websites surfed at Cyber Cafes", the Act was passed by the Parliament.

However without the notification of the accompanying "Rules", the Act could not come into immediate effect.

Finally it was announced that the Act would come to effect on August 15th and the Prime Minister would release the first digitally signed document during his Independence Day speech from Red Fort.

At this time, the Rules were yet to be announced and Controller yet to be appointed. The proposal was therefore dropped and instead, the

Government came out with a draft copy of Rules and posted it on the website of Ministry of Information Technology for public comments. It also called for public suggestions on the person to be appointed as the "Controller".

The rules were finally notified on October 17th 2000, after incorporating some of the suggestions made by the public and Mr K.N.Gupta was appointed the Controller of Certifying Authorities under the Act.

With this notification, Digital Contract Era in India was theoretically ushered in to the Country.

It however took more than a year and half from the date of this notification for the first Certifying Authority in India to announce its own Certification from the Controller of Certifying Authorities on February 7, 2002.

In the mean time, on September 4, 2000, another Act which falls in the realms of Cyber Laws, namely the Semi Conductor Integrated Circuits Layout-Designs Act, 2000 became law.

Even though the Information Technology Act was in force since October 17, 2000, the Government could not appoint the Adjudicating officers and Cyber Regulations Appellate Tribunal to administer the Act. Recently, the Government has under directions of the Mumbai High Court taken a decision to designate the IT Secretaries in every State as "Adjudicating Officers" Under the Act. The notification to this effect has been made on March 25, 2003.

Further the amendments to the Negotiable Instruments Act through Negotiable Instruments Amendments Act 2002 and the consequential amendments to ITA-2000 were notified with effect from 6th March 2003 bringing in the concept of Electronic Cheques to the Banking scenario.

With these legislations, India has started its journey into the field of Cyber Space legislation and the future course that these laws take will determine the way we live not only in the Cyber World but also in the Non Cyber World.

CHAPTER II

THE INTERNET ERA

Internet was theoretically born in the late 1960 s as a project of the US Defense Department. By late 1980 s the concept of Internet had taken firm roots in USA and parts of Europe through the educational institutions which were part of the initial Internet project.

To the public in India however, Internet was first launched in August 1995 by the then public sector Videsh Sanchar Nigam Limited (VSNL). Initially, Internet was accessible as a "Shell Account" which could be handled only by regular computer users who were familiar with the Command/DOS interface as distinguished from the "See and Click" interface (Graphic User Interface or GUI) with which we are familiar today in the Windows environment. .

A new revolution was however kicked off after VSNL started offering TCP/IP access to the public some time in 1997. This opened up the World Wide Web with its graphic interface to the Internet users in India. This also enabled the common man who could click his way through the Windows menu but was not comfortable with the DOS screen, to get onto the Internet. As a result, the usage of Internet started to grow at a maddening pace.

ONE HUNDRED AND FIFTY LAKH NETIZENS IN INDIA AND GROWING FAST

Since the introduction of the TCP/IP accounts, VSNL and other Internet Access Providers such as MTNL, Satyam Infoway, DishNet, Bharti Telecom, etc., have provided over 40 lakh Internet accounts in India by end 2002. Current indications as per ITU (International Telecommunication Union) estimation is that are that the Netizen population (Internet users) in India is around 165.8 lakhs (16.58 Million) in December 2002 marking a penetration of 1.6 % of the population.

.

World wide, there are estimated to be around 682 million Netizens marking 10.7 % penetration of the world population. Nearly 30 % of the Net users are in USA. Serving these 682 million Netizens are an estimated 35 million active domain names most of them hosting web sites with a huge volume of information on all aspects of life provision of communication services such as E-mail, Chat and Discussion Boards, and various kinds of Commercial transactions.

FALLING COSTS AND GROWING POPULARITY

With the advent of Web TVs and the ubiquitous Cyber Café's in all cities, even those who do not own a Computer can now access Internet. Soon there will be Internet Kiosks in all public places enabling the public to have quick sessions to view e-mails or browse the latest news.

Access of E-Mails on Mobile phones has also enabled the services of Internet to be available outside the traditional Computer based environment.

Several State governments have embarked on projects to take Internet browsing centers to smaller towns. With content now being made available in all Indian languages, it would not be long before Internet penetrates the rural market as well.

Internet access has already become very economical in India with the average access cost coming to about Rs 7.50 per hour. Access through telephone however costs an additional Rs 24 per hour making the total cost of internet access around Rs 30 per hour. Recently the telephone cost has been revised downwards so that Internet access cost through dial up connections in India has been brought to around Rs 15/- per hour on an average. For heavy users, there are access providers who provide leased,

DSL (Digital Subscriber Line), and Cable access on a monthly rental basis.

Thus the easy availability of the services, their utility to a wide section of the society and more than anything else, the falling cost of Internet access has made it a universal communication tool as common as the Telephone.

With Internet telephony having become legal in India, from April 2002, Internet has already become a "Long Distance Phone" with call rates which are around 1/10th of the current costs for International calls.

People today don't buy Internet access because they have a computer or the telephone. They buy the Computer because they want to access Internet.

INTERNET IS A WAY OF LIFE

As things progress, the adoption of Internet has increased so much that we wake up to see our morning news on the Internet, correspond through e-mails, retrieve information from web sites, Chat with our friends on line and listen to music or follow a Cricket match on the Net.

The advent of E-Commerce would mean that we may order Cigarettes or Grocery or do Banking or Share trading on the Internet.

While some have already adapted to this style of living, others are moving in this direction and the "Digital Divide" is narrowing at least in terms of access to Internet.

That's why we need to recognize that the immediate future before us is the Internet Era.

NEED FOR LAWS TO GOVERN THE E-SOCIETY

The unprecedented popularity of the Internet and its deep penetration into the common man's life brings in its wake a new social responsibility for administrators as well as those who are driving this Internet revolution. In order to bring order to the lives of Netizen population who live in a border-less virtual society, the governments all over the world led by the United Nations and the government of USA are evolving a regime of uniform "Cyber Regulations".

India has taken the first step in this regard by passing the ITA-2000 to define the Cyber Laws for India. This has redefined the business and legal process in the country by bringing in electronic documentation as a legally accepted replacement of written documents. This law will not only apply to Internet transactions but also to transactions over other Computer networks of Companies, Banks, Educational Institutions, and Government Departments etc.

TECHNOLOGY THAT DRIVES THE INTERNET

In order to fully understand some of the nuances of the proposed laws it is necessary to be familiar with some concepts that drive the Internet technology. Many of the readers of this book may already know something about Internet and its many uses. However, for the benefit of those readers who have decided to first understand what Cyber Law is, before studying the Internet technology, a brief introduction of the basic elements of Internet and how they function would be in order.

This will also be handy for the members of the legal profession who are being exposed to this new age where their familiar paper bundles may be replaced by floppies in the pocket.

HISTORY OF INTERNET

Internet basically started as a device to connect computers in far off places so that they can communicate with each other. This required usage of a common protocol (language of communication between electronic devices) for exchange of data and ability for connectivity without Cables. It was also considered critical that the computers should be networked in such a manner that they are capable of reaching each other through multiple routing paths. The idea was that in case of a nuclear war where some communication lines may get destroyed, the computers continue to reach each other through alternate routes.

These considerations were realized as a Defense Research Project in USA and the first Internet network started functioning by 1969 through a net work named ARPANET. (Advanced Research Project Agency Network). Initially the technology was a closely guarded military project. It was in the 1980 s that the education networks and other Government agencies in USA came into the Internet network.

INTERNET IN THE PUBLIC DOMAIN

Since the advent of 1990s, Internet has been brought into the public domain and has grown to become a vast Network of Networks consisting of millions of computers. The digital signals travel from the user's computer through telephone lines and satellite channels.

Every computer connected to the Internet network has a unique identification called the IP address. This is a number in four parts such as 202.54.6.20. The amazing technology called the TCP/IP sends and receives data packets from one computer to any other computer in the Internet through whatever path is available for the time being. In so doing, the message is broken up into little packets and sent from one node to other in the network until the destination computer is reached. The

packets get reassembled at the destination re-creating the original full data packet.

Yet another complementary technology called Hyper Text Mark up Language (HTML) has enabled data to be presented as pages with "Hyperlinks". These hyperlinks can be assigned to a specific text in such a manner that, if you click on the link, a search and retrieve-routine is triggered for the linked file wherever it is situated on the network. The individual computers are equipped with software called the "Browser" that reads the documents created in this language.

THE EMERGENCE OF THE WORLD WIDE WEB

These developments have encouraged some persons to keep their computers permanently connected to the Internet and let people connect to their computer and see pages created by them. This has given rise to the concept of "Web Servers" where "Web Sites" are presented to visitors. Each web site is a collection of web pages suitably interconnected for navigation. Such sites can be accessed from any computer connected to the Internet by simply typing the address or the URL (Uniform Resource Locator, e.g.: http://www.naavi.org) in the browser window.

This is essentially the World Wide Web or the WWW network of browsable web content. Today there are nearly one billion (100 crore) such web pages and about 35 million (3.5 crore) active URL s on the network containing information of various natures such as education, entertainment, business, philosophy etc.

KEY CONTRIBUTORS TO THE INTERNET REVOLUTION

Internet is a project for which contributions have been made by many. In future also, it will grow with the contributions of many ordinary persons working behind scenes. Yet, it is necessary to remember at least the three

most important visionaries who made Internet possible. They are Vincent Cerf, Tim Berners Lee and Jon Postel.

Dr Vincent G. Cerf of the University of California, Los Angeles (UCLA) is credited popularly as the "Father of Internet". He was one of the four members of the "Net Working Group" involved in the early days of the ARPANET project and co-designer of TCP/IP protocols.

Dr Tim Berners Lee, an Englishman working as a software consultant at CERN (the famous European Particle Physics Laboratory in Geneva) is credited popularly as the "Father of the World Wide Web". In 1990 he created the Hyper Text mark Up Language (html) and Hyper Text Transfer Protocol based on which documents could be shared by different computers. He also developed the first browser software to read documents written in html and called it the WorldWideWeb. He also set up the first web server known as "info.cern.ch." at CERN.

Dr Jonathan B. Postel, who also worked in the ARPANET project, can be considered the "Father of Internet Address System". He was the person responsible for maintaining the IP addresses of the Computers in the ARPANET and his system evolved into the Domain Name Registry system in due course.

MORE FACETS OF THE INTERNET

Internet also provides "Chat Rooms" where the user can exchange real time notes with others as if he is chatting with people in a real-world room. He can leave messages in a message board which others can visit at different points of time. He can send voice messages across as e-mail or even do voice chat on the Internet. If adequately equipped with a camera and a good connection, he can even run video-conferences over the Internet. All these and more have made Internet an all purpose multimedia communication tool capable of exchanging text, audio and

video messages across people sitting in different corners of the world.

The advent of Instant Messengers from MSN, Yahoo, and Rediff, India Times etc has added yet another novelty of people belonging to a community getting instantly notified when a fiend comes on line in some part of the globe.

ADVENT OF E-COMMERCE

Over the last few years, the technology of creating interactive web pages where Netizens who "Surf" this huge ocean of information can interact with the web servers on a real time basis, has given rise to commercial transactions being concluded during such visits. This development of E-Commerce has converted World Wide Web into a global marketing place. E-Shopping, E-Banking, E-Stock Trading have all taken firm roots in a Netizen's life. E-Education, E-Medicine, E-Gaming, E-Movies etc make it possible for a Netizen to use Cyber Space for most of his social interactions.

THE PROCESS OF SHOPPING ON AN E-COMMERCE SITE

An E-Commerce site essentially consists of a product catalogue and an online payment mechanism besides the information that is normally contained in a website.

If the site is having a large number of products on sale, the customer will be provided an option to go round the e-shop, select products he wants to purchase and put them in a shopping cart/basket.

On confirmation of the intention to purchase, the customer gets an online invoice.

At this point of time the customer will be prompted for payment. If the site has made arrangements for accepting credit cards the customer will complete the necessary form where the card number, expiry date, name of the holder etc will be filled up and submitted for payment.

The site will then refer the card details to the "Payment Gateway" manager who verifies the card on line with the master data base of cards and provides authentication.

Once the authentication process is over, the shopping session gets concluded and the shopper may leave the site.

The E-Commerce site owner, on receiving the authentication of the payment makes arrangement for the shipment of the goods.

Based on the authentication, the Bank participating in the payment gateway, will pay to the merchant and claim reimbursement with its commission from the card issuing Bank.

Some of the paying Banks insist that the payment would be released to the merchant only after the order fulfillment confirmation is received in the form of a shipping note signed by a reputed shipping agent.

With such an arrangement, a website can effectively display products and collect money on line. If the product to be delivered is a "Digital Product" such as software or a "Music file", the product can also be delivered online.

TYPES OF E-COMMERCE SITES

If a web merchant is selling products to a consumer on the net, the transaction is often referred to as B2C E-Commerce, meaning Business to Consumer.

An auction site where a person can become a member and then offer his products for auction enables a "Consumer to Consumer" sale and is referred to as C2C E-Commerce.

A site where transactions between Business to Business are envisaged is similarly referred to as B2B E-Commerce. Inter Bank transactions or Inter Company transactions fall into this category.

With the facilities of information delivery and payment combined together, Internet has today become a place for Communication, Entertainment, Education, Entertainment and Business. As days pass, the versatility and utility of Internet is increasing at such pace that the Virtual world is converging onto the Real world.

The Future of Business is E-Business

Today the use of Internet in Business is so wide spread that the statement "There is No Business Without E-Business" is no longer the optimistic dream of an E-Business Consultant. It is the reality.

The evolution of E-ways of doing business is itself a matter of interesting study for management practitioners.

The initial use of Computers in Business was as a "Digital Aid to the Secretary" in replacement of the electronic typewriters. It made the work of drafting of letters easy. Next it was the finance and personnel departments in Companies which adopted Computerized ways of account keeping and salary records maintenance.

However, as long as Computers remained as single desktop machines, their role was only to assist the operators. It was with the evolution of "Networking" that "Communicating Computers" emerged in the office environment and people started transacting in the Cyber Space created by the networked computers.

While the development of LANs and expansion of their functionality is a continuous development, a paradigm shift in the use of Computers came when the Corporate network got connected to the outside world through Internet. Simultaneously, development of large Intranets and Extranets expanded the use of Computers in to a "Knowledge Management Tool" and "Productivity Enhancement Tool".

However it was the ability to do transactions on the internet (E-Commerce) that really changed the perspective of the Computers in corporate business. It all started with the Electronic Data Interchange system (EDI) which enabled the exchange of documents from one Computer network to another often through proprietary gateways. The emergence of TCP/IP as a universal protocol and HTML as a universal document language opened up an EDI process without proprietary tools.

In this open network environment, "Security" was a critical issue. The security in the initial stages was to ensure that there was no "Eaves Dropping" or "Data modification" during transit. But as the dependency on E-Commerce grew, there was need to integrate E-Commerce into the legal framework by making "Authentication", an integral part of data interchange and "Legal non-repudiability", and an essential part of such communication.

It was in this context that one of the main objectives of the Information Technology Act-2000 was set to promote E-

Commerce by providing a safe environment for exchange of electronic communication over open networks.

Today, the IT enabling of business has taken such deep roots that we often refer to an environment of "E-Business" rather than "E-Commerce". In the E-Business paradigm, every aspect of business from Finance, Marketing, Purchase, HRD etc are conducted using electronic documents. From receiving an application for recruitment to getting the firing order or submitting a resignation, an employee of the Company deals with E-Documents.

Hence the role of Cyber Laws has grown multifold and Cyber Law Compliancy has become an integral aspect of "Quality Process" in a business entity.

In the initial days of E-Commerce, the business strategy development in Companies was to use the Web as a means to extend their real world business.

In between, some aggressive players came up with the concept of Dot-Com business where the entire business was created, established and maintained in the virtual world. The example of Network Associates Inc in the domain name business, Amazon in the Book Business, Napster in the Music Business and a couple of Virtual Banks made Dot-Com business model, a dream for small entrepreneurs. With a global reach through a small web site, the dot-com model enabled "Knowledge Capital owners" to take on "Finance Capital Owners" in the area of "Service" or "Customized Products".

The rapid growth of the dot-com concept and the support of the venture capitalists created a thriving Internet Economy that shook the real world giants.

To counter this threat, the real world operators first started promoting a concept where the strengths of the "Brick and Mortar Business" developed by them over a period could be leveraged with the advantages of Internet. This was aimed at developing a "Trusted and Customer Friendly" business model under the nomenclature of "Brick and Click Model".

Soon however, the natural survival instincts of these real world masters gave birth to a new business strategy aimed at killing the emerging competition from the Internet Economy Players.

The real world lords, who wanted to consolidate their position in the market, systematically developed an "Anti Dot Com" sentiment working around the security problems inherent in the Internet environment. They also used "Cyber Laws" as a tool for stifling the Internet Economy initiatives. Napster is a classic example of this strategy.

Thus Copyright and Patent Laws are being invoked today to threaten "Hyper Linking" or "E-Commerce", Trade Mark laws are invoked to threaten Domain Name Bookings, and Privacy laws are promoted to stifle Online advertising revenue of content portals.

On the positive side, the development which supported the Virtual Business Place was the "Digital Signature" and "Biometric Authentication Systems" which brought a semblance of respect and safety to Internet communication.

As a result of all these developments it is no longer sufficient to structure the E-Business strategy today either as an extension of the Brick and Mortar Business or as a stand alone Dot-Com business.

E-Business as the Hub:

Successful business strategy in today's business is therefore to treat E-Strategy as the Hub of the total business strategy. It is immaterial whether E-Business exists from day one of the business or not. The perspective business plan must include the "E-strategy" before the laying of the first brick for a factory or business.

In such a strategy, the Internet presence of the Company is the fulcrum for all communication dissemination to customers as well as channel partners and staff.

In such a strategy,

- The planning of Marketing and Distribution will be dovetailed to support the web initiative rather than the other way round.

- The Finance strategies are developed based on the virtual asset portfolio in addition to the physical asset portfolio.

- The HRD strategies have to factor the possibilities of the e-mails of top executives being misused to spread false rumors on some employees or to expose misdeeds.

- The Supply-Chain management and CRM (Customer Relations Management) also is dependent on what the Web can achieve.

Thus every aspect of business starts with what the web strategy can achieve and how it needs to be supported.

If it is possible for the Board members to meet in the virtual place more often than physically, the Board meetings need to be enabled for Virtual conferences. Similarly, shareholders can be provided virtual voting rights so that they can participate in the management more freely than otherwise.

This is the future scenario of Business to which all of us need to keep ourselves ready. The first step in this direction is to build an awareness of the "Cyber Laws" within all levels in an organization, develop "Digital Signature Capability" and develop Corporate policies for defining the norms for their employees for dealing with the Cyber Space transactions. As regards Software industry, it is all the more necessary to understand the Cyber Law implications of software they develop and deliver to their customers.

E-Business therefore is the future face of Business and Cyber Laws will be the life blood of the industry. Sooner we realize this, and equip ourselves, better it is for us.

CHAPTER III

ELECTRONIC DOCUMENT

In India, Information Technology Act-2000 (ITA-2000) which became effective from October 17, 2000 is the legislation which has brought legal recognition to Electronic documents for the first time.

ITA-2000 has taken the Indian society from a paper based society to an electronic document based society by categorically mentioning that except for a few exceptions,

> Where any law provides that information shall be in written, typewritten or printed form, the requirement is deemed to have been satisfied if such information is rendered in electronic form and accessible for future reference (Section 4).

EXCEPTIONS

According to section 1 of ITA-2000, the provisions of the Act will not be applicable to

- ✓ **"Negotiable Instrument"** (other than a Cheque) as defined in the Negotiable Instruments Act, 1881
- ✓ **"Power of Attorney"** instrument as defined in the Power of Attorney Act, 1882
- ✓ **"Trust"** as defined under the Indian Trust Act 1882
- ✓ **"Will"** as defined in the Indian Succession Act 1925 and
- ✓ **"Any contract of Sale"** or **"Conveyance"** of Immovable property.
- ✓ **Any other document** or transaction that may be notified by Central Government.

When the Act was first brought into force, Cheques were also exempted from the provisions of ITA-2000 along with other Negotiable Instruments such as the Bill of Exchange and the Promissory Note. However, in December 2002, the Negotiable Instruments Act 1881 was amended and two new categories of instruments referred to as "Cheque in Electronic Form" and "Truncated Cheque" were defined. Simultaneously, ITA-2000 was also amended to delete "Cheques" from the category of exempted instruments mentioned under Section 1 of the ITA-2000. The notification became effective from March 6, 2003.

The Act also states that

> Where any law provides for the filing of any form, application or any other document with any agency controlled by the Government, such requirement may be effected in electronic form. (Section 6)

The Act also further states that

> Where any law requires maintenance of certain records (Ed: by a Government Agency) for a specific time or permanently, it would be enough compliance of the provisions if the record were kept electronically. (Section 7)

It is to be noted however that the use of electronic documents by the departments of the Government and the Ministries at the Central and State level has been left for the present as an option that can be exercised by such bodies and not an obligation that can be enforced by the citizens. (Section 9).

The omission of some of the categories of Instruments from the applicability of the Act has been debated often. Apart from the fact that at the time of first enactment of the Act, the

Government felt that the market was not ready to accept Electronic Documents as replacement of instruments such as Cheques, the lack of a mechanism to collect Stamp Duty on Electronic Documents was also a reason for keeping certain documents outside the purview of the Act.

AMENDMENTS TO OTHER ACTS

The act has also simultaneously brought amendments to a few other acts such as Indian Penal Code, Indian Evidence Act, Banker's Book Evidence Act, and Reserve Bank of India act to provide recognition of Electronic documents in the respective areas covered by these acts.

These provisions provide a universal (Save the Exempted Categories) recognition to the Electronic documents and make them part of the everyday life of an Indian citizen whether he is also a Netizen or not.

THE DIGITAL TRANSFORMATION

Basically, Presentation of information on paper enables easy grasp of complicated thoughts. In the context of entering into legally valid contracts,
Use of written instruments provides the following key advantages.

- Authentication by Signature
- Non-Repudiation by contracting parties
- Confidentiality during Transmission
- Integrity of data During Transmission

However, the world has now moved from the use of paper based document creation to use of computers in most of the routine

writing work.

It has become common today for documents to be mainly created on a computer and stored in digital form. They are also transmitted in digital form and read on other systems. Finally they may be deleted while in digital form itself completing the entire life cycle of a document in digital form only. Documents are printed and converted into paper form only if necessary.

Digital form has therefore become the primary form of document handling while the print form has become the "Back up" form or the secondary mode of document handling. The legal and judicial system therefore has to take this change of societal norms into consideration when they apply law in this emerging digital society.

Technology can also be configured today to simulate most of the specific patterns of usage of paper in our administration on the electronic documents. For example, in a Government department, if the paper has to move from one person to another incorporating their comments, software can enable the document to move from one message box to the other in a predetermined sequence and comments and signatures can be tagged along. If necessary, documents can be circulated over the Internet or a secured Virtual Private network to remote locations and comments picked up as if the file is being passed around to different tables in the office.

As a result, it is possible to replace the need for paper based documents by electronic documents in most of our transactions.

THE DEFINITION OF AN ELECTRONIC DOCUMENT

What was so far holding up the transformation of our day to day life from the paper-based system to a digital record based system was the absence of legal recognition for the digital document. ITA-2000 has therefore taken steps to define "Electronic Records", and related aspects of Signature, Storage, and Admissibility in evidence etc.

An "Electronic Record" is defined in ITA-2000 as a record generated, stored, sent or received by electronic means and includes data, image, or sound.

The basic form of an electronic record that we can visualize is the text form in which letters or other pieces of communication are expressed. An e-mail, a web page, a Word document etc are examples of electronic documents. But the definition is broad enough to include pictures, photographs, audio and video files as well as any set of computer instructions constituting a program.

The electronic records are stored in electronic devices such as hard disks of computers or other storage devices such as Floppies, CDs etc. Today, it is becoming common practice to store electronic data in information servers that can be accessed from remote locations through Internet. Many of these records are even created and retrieved as voice packets through a telephone line.

Irrespective of the form of the document, in technological terms, an electronic document is nothing but a collection of bits and bytes. A bit is an electronic switch which is either in an "On" state or an "Off" state. A group of bits constitute a byte. A group of bits and bytes in a specific sequence represent a character

(letter, number etc) or a Word. Similar aggregations create the document or even a picture, an audio and video document.

Every electronic document is therefore a "Number" constituting a series of '0' s and '1's. It can be treated as a mathematical number and be subjected to manipulations such as addition, subtraction, multiplication, division, factoring etc.

WEB FORMAT IS THE UNIVERSAL DOCUMENT STANDARD

It is also necessary for us to understand that electronic documents are created and used with an application and a relevant operating system. Just as a document written in Japanese cannot be normally read and acted upon by some body in India, a document created in one proprietary system may not be normally readable in another system. Worse still, the document maybe wrongly read in another system which is slightly incompatible.

All reference to electronic documents in a contract therefore is complete only if their format is also defined.

When electronic contracts create liabilities that make it necessary for one or more parties to create and transmit further electronic documents, (Say notices or performance reports etc), it becomes necessary to specify the formats in which such documents are to be created.

Alternatively, if a document has to be widely accepted, it becomes necessary to eliminate this system dependency. Since Internet uses platform independent protocols, it is an automatic choice as the de-facto standard for all digital activities. A document which is "Web–Enabled" may therefore be a universally accepted format while other proprietary formats may not necessarily be so.

Web enabling means that the document must be reproducible using a normal "Browser Software" in a form that is exactly what the creator of the document intended. The need for special plug-ins or even rare fonts to read the document should preferably be avoided in digital contract documents.

ITA-2000 has not dealt with standardization of document forms in digital contracts. But when cyber evidence has to be presented in courts in future, this aspect will be critical. If a document is created in a format which uses exclusive software and the particular version of the software required to read the document correctly is no longer available when the evidence is presented in the court, the admissibility of evidence may be jeopardized. (e.g.: E-Book format created with software from a company which has ceased business.)

The underlying principle in use of Electronic documents is that "An Electronic Document is a Document only in a compatible system and not otherwise".

In all our discussions through out this book, we have presumed the Internet as the basic network for document distribution even though ITA-2000 covers activities not only on the Internet but also other Proprietary networks within an enterprise. Even these systems today use web formats for many of the shareable documents.

LEGALLY ACCEPTABLE ELECTRONIC RECORDS

Creating electronic documents that are legally acceptable actually involves a high degree of technological complexity.

For an Electronic document to pass the test of legal acceptance, it has to provide adequate substitutes for each of the advantages of a paper-based document such as ability to be authenticated, to preserve confidentiality, to preserve data integrity during transmission and storage and provide for non repudiation by contracting parties.

If a legally sensitive statement or a picture is being used as an electronic document, just as every dot and comma is relevant in a printed document, every bit and byte needs to be preserved without loss or damage or manipulation. It should also identify the signatories to the document in a manner that any of them would not be able to deny their consent to every bit (digital) of the document. The documents should also be able to be transmitted in confidence and stored securely.

One of the ways by which an ordinary digital record can be secured is to digitally stamp in such a manner that even if it falls into wrong hands, it cannot be altered without the genuine user of the document knowing it. This process is referred to as "Digitally Signing" the document. (This process has been explained in greater detail in the chapter on "Digital Signatures").

Once a document is digitally signed, it is as good as any other paper document carrying the signature of the person creating the document. It can also be transmitted in confidence so that it cannot be read by anybody other than the intended addressee. It can also provide assurance against any alteration after leaving the

hands of the originator of the document. It can be therefore be used to create Electronic contracts that can be defended in a court of law.

SOME EMERGING ISSUES

For legal clarity, it is essential to distinguish Electronic Records from other kinds of records which are apparently similar. For example, an e-mail can be sent either as a text or as a voice mail. Both are "Electronic Documents" subject to the provisions of ITA-2000.

Similarly, an audio file can be recorded both on a magnetic tape as well as a CD. The record on the CD is an "Electronic Record" as defined in ITA-2000. The audio tape is however outside the scope of the ITA-2000.

Similarly, the video captured on a digital camera or stored on a CD is an Electronic record while a picture on a "Film" is not a digital picture.

A song recorded for a movie is digitally produced at the time of its creation. It may then be converted into an audio tape. Here, if there is a "Copyright issue", what is applicable to the original document is "Copyright of an Electronic Document". On the other hand, the audio tape becomes an adapted work in a different media.

An SMS message on a mobile phone is an electronic text message and is subject to the provisions of the ITA-2000 while the voice transmitted on an analog telephone line may not be so.

Voice or Video transmitted on a "Digital Line" is "Electronic Documents" whether or not they are stored or not. When a cable

TV is transmitting a digital video image, there are a series of electronic documents being displayed on the TV screen just as a video file is seen on a Computer screen.

In the case of a digital video or audio transmission, the transmitted data may not be recoverable at the user's end after they are displayed. This is equivalent to a situation where the temporary Internet files are deleted instantly and there is no cache memory on a Computer.

These are some of the issues that will be confronting the legal community in the coming days of Convergent technologies and lead to interesting interpretations.

Electronic Documents and Cyber Space- A thought for Cyber Jurisprudents

(Ed: This is a thought for the development of Cyber jurisprudence and not necessarily for interpreting the clauses of the Information technology Act 2000.)

The set of laws discussed in this book has been termed Cyber Laws even though some refer to such laws as Computer Crime Laws or E-Commerce Laws. The choice of the word Cyber Laws is deliberate since the set of laws discussed here cover the life and property of persons living in Cyber Space.

The use of the concept of "Cyber Space" to describe the domain where the laws are applicable and the term "Cyber Society" to describe the people who are the subject of these laws provide a clarity that no other approach provides for understanding these laws.

We should appreciate the vision of novelist William Gibson who is credited for the first use of the term "Cyber Space" in his novel Neuromancer to describe the imaginary transaction space in which the hacking community operates.

Cyber space concept as we shall use in our discussion springs into existence when two electronic devices start communicating.

For example there is no Cyberspace when a single computer is being used by an operator to say create documents or for carrying out calculations. However when another computer gets connected with the first computer and they start communicating with each other, the Cyber space is created.

The Cyber space acquires an even more distinct form when millions of Computers are simultaneously talking to each other in the Internet.

This Cyberspace cannot be touched or felt but can only be experienced. It is that place where the online chat is taking place or a person is viewing the web page or where your e-mails traverse.

One of the critical features of this space is that one enters this space using the real world devices such as a Computer but we cannot say that Cyberspace is created by the hardware and software in the user's computer.

Even though one can keep a snapshot of the Cyber space transaction in the form of downloaded files in the user's computer the transaction itself vanishes the moment the user disconnects the communication channel.

Electronic documents are the interactive manifestations of the Cyber transactions. They exist only in relation to the Cyberspace. (ITA-2000 however considers even print outs from Computers as equal to Electronic Documents for the purpose of Indian Evidence Act)

Dr Einstein explained his "Relativity Theory" by stating that all physical laws are real only with reference to a "Fixed Frame of Reference". They would be different if the frame of reference is changed. Similarly, for Cyber Electronic documents, Cyber space is like a "Frame of Reference". If this frame of reference is not present, then the electronic documents have no existence.

Just as Einstein used the concept of "Frame of Reference" to describe the laws of physics, we shall use the "Cyber Space" concept to describe the laws of Internet transactions.

Yet another concept from Physics that explains the role of Cyber Space is the proverbial medium of "Ether" which helps explain many of the real world phenomena. Just as the Debroglies's matter-wave theory of physics establishes the link between the existences of matter to the vibrations of the medium of Ether, the existence of Cyber Properties are best explained by assuming that there is a Cyber space which supports the formation of Cyber Properties.

The virtual properties we talk of in the Internet space such as the Domain Name, Web Space, Content on a website, Web Utility Software etc, have no meaning unless we pre suppose the eternal existence of the Cyber space. Similarly, the digital personality represented by an e-mail address say naavi@vsnl.com has no meaning if the e-mail system vanishes along with the Internet. If the digital person Naavi had any internet property or right, all that would stand liquidated with the vanishing of the Cyber space.

It is in this context that we can say that all virtual properties and personalities have value and life only "Relative" to the Cyber space. This "Relativity Theory of Cyber Space" helps us understand many problems involved in the collection, production and proving of Cyber Evidence in a Cyber crime scenario.

For example, in a crime such as an "Attempted Unauthorized Access to a Network", the evidence will mostly be transitory and vanish the moment the attempt is stopped. The judiciary should therefore accept this position as the nature of Cyber society and act accordingly.

Many of the legal and jurisdictional disputes that arise on the Internet can be better understood and handled if we accept the existence of Cyber Space and treat the Cyber society as a different society with its own culture, population and property. A fall out of recognizing the existence of Cyber space is the necessity to define its relation with the Meta society.

It may not be ideal to consider as if all virtual properties are real world properties and all virtual identities have to match real world identities even though this is the popular concept now prevailing. The two can be considered distinct as long as there is no overlapping of effect.

However, any inter society dispute between the Cyber society and the Meta Society can then be resolved like how we resolve a dispute between two different countries. The Intra-Cyber Society disputes can however be settled by the Netizens through its own democratic process where digital persons elect digital administrators to manage the digital society.

Many of the legal disputes get complicated because we try to define the Cyber space as an extension of physical space as if India has an Indian Cyber space and Pakistan having a Pakistani Cyber space.

While technically it is possible to restrict access to different areas of Cyber space through Internet gateways and thereby create artificial Cyber boundaries linked to geographic boundaries, it would be better to let the Cyber space develop as a global virtual nation.

We can then look at Cyber Laws as a means of harmonious living of Netizens rather than a means of protecting the Meta Society

properties. Presently, most Cyber regulations are conceived by treating as if Netizens are interested in stealing the possessions of Meta society property owners who need to be protected.

ICANN has already shown how Cyber Democracy can be built and nurtured through its At Large membership. This type of Cyber democracy of the Netizens, by the Netizens and for the Netizens is the ideal means of regulating the Cyber space.

CHAPTER IV

DIGITAL SIGNATURE

With the advent of the Electronic age and a drive towards a paper less society, it has become necessary to enable people exchange electronic documents in such a manner that the documents can be identified to have been issued only by the person named therein as the "Sender" and contains "all" but "only" such information that the sender intends to send.

The key element in this process is to generate a signature equivalent to what we know as "Signature" in the Paper society which authenticates an electronic document, certifies the contents as what they are intended to be and binds the signatory to the statements made there-in.

In order to understand how ITA-2000 proposes to achieve this, it is necessary to briefly analyze the import of "Signature" in the paper society. This will enable us understand the concept of "Digital Signature" in the required perspective.

SIGNATURE IN A PAPER BASED SOCIETY

Signature is the basis of all transactions in the paper-based society. Even though Oral Contracts are valid in law, it is an established practice to reduce agreements to writing and affix signatures, so that the intentions of the parties to the agreement are easily verifiable by a third person in case of dispute.

The concept of "Signature" covers the writing of one's name in whatever language, whether legibly or otherwise. Thumb impression is an alternate form of affixing consent to a document

and also completes the process which a signature is normally expected to do. For Corporate entities, affixing of the Common Seal amounts to a "Signature". The affixing of the Common Seal is also normally backed by the signature of a person authorized to affix the common seal.

Even though the entire paper based society is dependent on Signatures, it is interesting to note that these are not unique and actually may vary with the passage of time.

In India we also have the practice of affixing signatures in different languages, a practice recognized even by the Government in Currency notes. Despite these shortcomings, writing of name in a running handwriting is the popular form of affixing signatures to documents.

When a signature is affixed by a person other than the person it is purported to represent, it becomes a forged signature even if it is indistinguishable from the original. On the other hand, a signature written by the same person in a different style or language doesn't constitute a forgery and can bind the person as effectively as his normal signature can do.

It is clear therefore that even though signatures are generally compared for visual matching, more than the form of signature and it's matching with the original, what matters in law is the person who has affixed it.

When you encounter a Banker or a Post Master refusing to accept your signature as yours because it does not tally with the specimen, remember that they are actually relying on the procedural requirement rather than the legal requirement.

Yet another point that is important to validate the writing of name as a "Signature" is the intention of the person who is signing. The legal system in India presumes that a person who has put a signature to a document understands and agrees to what is written therein and binds himself to a legal liability arising there from.

The signatory is however free to prove in the court of law that either he was not in a sound state of mind or was otherwise prevented from understanding and applying his mind to the contents of the document at the time of signing and contend that he is not liable under the document. It is left to the Court to examine the circumstantial evidences and come to the conclusion as to whether the "Purported Signature" is in fact a "Signature" or not. There are several instances where the Courts have come to the conclusion that a signature is in fact not a signature since it was obtained by Misrepresentation or Coercion or when the signatory was in an inebriated or unsound state of mind or because the contents were tampered with after the signature was affixed.

Thus, even though we recognize the "Writing of the name in a consistent manner" at the end of a written statement as a "Signature", the essence of "Signature" is the intention to express agreement to what the document above the signature contains. If there is no intention to agree to the document, mere writing of the name or a thumb impression does not constitute a signature.

It is for this reason that when a thumb impression is taken as a "Signature" or when the document is in a language different than the language of the written signature, an independent witness is made to add his certification that the "Contents of the document were read out to the person affixing his signature/thumb impression and he has understood the same before signing".

SIGNATURE IN DIGITAL SOCIETY

The term "Digital Signature" applicable for the Electronic Document has been defined for the first time in the Indian Statute through the ITA-2000.

The purpose of the "Digital Signature" is

- To identify the originator of a message/electronic record,
- To indicate approval of the originator to the message, in a manner, that is reliable enough for a third party to verify and confirm that
    - the electronic document could not have been created by anybody other than the originator and that
    - the document could not have been tampered with by anybody after leaving the originator.

The concept of Digital Signature is built on the technology of Secured transmission of electronic documents over a Computer network. In order to appreciate the nuances of the concept of Digital Signature provided in the ITA-2000, let's try to first get a grasp of the Risks attached to and Technical aspects involved in the transmission of electronic documents over a Computer network.

TRANSMISSION OF ELECTRONIC DOCUMENTS

An electronic document as we already know consists of a sequence of bits representing the state of electronic switches, which can be either on or off. Any electronic document is therefore a set of bits in a particular sequence.

When such a document is to be transmitted within a network, it moves from the originating computer through a cable (or wireless signal) to another computer to which it is addressed. When there are many computers available in a network, it may be necessary for the signals to be passed through routers which are like junction boxes. When Signals reach here their addresses are read and the signals routed to the appropriate channel. When signals travel over the Internet there will be many such nodes through which the signals pass before they finally reach the destination.

Also, under the TCP/IP protocol, which runs the Internet, the document to be transmitted, is broken up into several smaller data packets before they are addressed and despatched. These packets may take different routes to reach the stated destination and may reach at different times (all within a fraction of a second of course). At the destination they are arranged into the original sequence to re-create the original message.

In view of this method of transmission of data, it is quite possible that some of the data packets may be lost in transit or may reach wrong destinations. Alternatively, somebody may steal the data packets on the way and try to read the message. Such an interceptor may try to impost as one of the parties to the contract and modify the terms otherwise agreed to between them.

In order to maintain the confidentiality of communication, it is therefore necessary to send the data in an "Encrypted" or "Coded" form so that if it falls into wrong hands, it cannot be understood. Obviously, the receiver of the message should know how to decipher or "decrypt" the message so that he can see the message in the original form. This is called the science of Cryptography and is the backbone of the Digital Signature system.

The science of Cryptography is used along with the complimentary technology of "Hash Functions" in designing a Digital Signature System.

There are two types of Crypto systems. The conventional form called "Symmetric Crypto system" and the more secure "Asymmetric Crypto system".

SYMMETRIC CRYPTO-SYSTEM

Under this simpler form of Cryptography, there will be a "Key" known both to the sender and the receiver which can encrypt or decrypt the message. This type of single key encryption is called "Symmetric Key Encryption system".

The basic encryption process will systematically transform the original sequence of bytes in a document into a different set and when decrypted, will yield the original sequence once again.

HASH FUNCTION

Hash Function is another important constituent of any Digital Signature process meant to ensure "Data Integrity". It assures that even if a Comma or a Space is altered in the original document it is found out.

The "Hash Function" will parse the document and produce a unique value referred to often as the Hash Code or hash Value of a document. This is indicative of the original sequence of bits and bytes in the message, which gets altered if the message is changed even by a dot or comma.

When the addressee receives the message, he would re-compute the hash value of the message and tally with the hash value that has been reported by the sender.

A Standard hash algorithm used in the digital Signature process is a "One way Function" which produces a hash code from a document but it is impossible to reconstruct the document from the hash code. It is also consistent that any number of times the algorithm is applied on a given document, the same hash code is generated. At the same time even if a comma or space is altered, it produces a different hash code.

Thus the Hash code system can ensure that the message has not been altered after it was despatched by the sender.

Here is an example of how a Hash Function operates.

Let's take the sentences

1. Here is an example of how a Hash Function operates.
2.: Here is an example of how a Hash Function operates
3. Here is an example of how a hash Function operates.

If we apply the hash algorithm MD5 to each of the above sentences, the result would be as follows:

(1) a62970c3bfe16618ad6b447b7eae6cc0
(2) 7de5facd44457efe8dbff60bd3cefbda
(3) be2f89ed4b3b1cd316e726d742613fee

As we can observe, the above hash codes are completely different from each other even though the difference from the first and second sentence is only removal of a full stop (period) at the end

of the sentence and the difference between the first and the third sentence is only a changing of the letter H in "Hash" in to a lower case.

This demonstrates how "Data Integrity" between two documents can be verified using the hash codes.

One may also note that all the three hash codes are of equal length and this would be so even if the parent document is any other large electronic file.

DEFICIENCIES OF THE SYMMETRIC KEY SYSTEM

While the symmetric key system of encryption ensures confidentiality of the message during transmission, since the same key is used for both encryption and decryption, the key needs to be transmitted from the sender of the message to the receiver. This exposes the system to the risk of Key theft.

Also, under this system, since the same key is shared between the sender and the receiver, a third party or (the judiciary) cannot conclusively determine whether an encrypted document was created by the sender or the receiver.

ASYMMETRIC CRYPTO SYSTEM

"Asymmetric Crypto system", also called the "Public Key Infrastructure (PKI) System" is an alternative system that overcomes the weaknesses of the conventional Symmetric Crypto system. This system uses two keys. Both are initially created by the originator of the document. One key is always held by the originator and is called the "Private Key". The other is distributed

publicly to any one to whom the originator has to send a secured message. Any message/document can be encrypted with one Key and decrypted with the other Key.

The two keys are different but form a unique pair such that every time a document is encrypted with the first key and decrypted with the second key, the original document is faithfully re-created.

If any encrypted document can be successfully decrypted using the Public Key purported to be belonging to the sender, it is reasonably certain that the document must have been encrypted using the private key corresponding to the public key. Since no body other than the sender is expected to possess the private key, it can be reasonably presumed that the sender alone has created the document.

Similarly, when a document is encrypted using the public key purporting to belong to a certain person, it can only be decrypted with the corresponding private key which should be in his private possession. Such a document cannot be read by anybody other than the private key owner.

Let us now see how a standard cryptographic algorithm such as the RSA (Acronym of the founders Rivest, Shamir and Adleman) functions.

Let us take the sentence "This is a test message" And encrypt it using RSA algorithm.

The resulting Cipher text would look as follows.

01c952e5ea7b0e01c836b02e9f33bc33016fe121bb174f609e
976aa5f8541c41

If this is decrypted, the original message would be generated.

For the purpose of decryption of a message such as above which has been encrypted using the private key of a person, one needs the corresponding public key.

The public key is a two element variable and a typical Public key can be expressed as follows.

m = 01d7777c38863aec21ba2d91ee0faf51 e = 5abb

Normally these parameters are contained in a file with an extension such as .key which the PKI enabled application can recognize and extract into its processing system.

The encryption process is for maintenance of confidentiality of the information while Hash code is for checking the data integrity. They are used in conjunction for the Digital Signature process.

The "Hash" function can also be used along with the encryption with the asymmetric key system to verify that the message has not been altered after it has left the sender.

Thus Asymmetric Crypto system in conjunction with the "hash function" can be used to determine the identity of the originator of an electronic document as also maintain the document's integrity and confidentiality during transmission. Since a third party such as the judiciary can apply the public key of a person to check whether an encrypted message was in fact encrypted with the private key of the subject person, the system also provides for non-repudiation. It therefore provides all the requisite qualities needed to constitute a "Signature".

Hence the concept of "Digital Signature" itself is developed on this asymmetric crypto system and also recommended under ITA-2000 as the only means of "Non Repudiable" authentication of an Electronic Document.

THE DIGITAL SIGNATURE PROCESS

In practice, the system of Digital Signature operates as follows:

The sender of a document uses one of the standard asymmetric Crypto systems that has the approval of the legal system and generates a key pair for the encryption of a document.

He then reaches the public key to the recipient in a manner by which the receiver knows that it could not have been sent by any body other than the sender. (This process is explained in greater detail in a subsequent chapter).

The sender then proceeds to create a "Hash Value" to the document and encrypts the hash value with his private key.

He then sends the message along with the attachment containing the encrypted hash value.

The recipient applies the public key of the sender to decrypt the encrypted hash value received by him along with the message. He also separately calculates the hash value of the message received by him using the same standard hash value generating software used by the recipient. If the two hash values tally, it means that there has been no change in the document as sent by the sender and as received by the receiver.

Since the encrypted hash value could be decrypted with the public key of the sender, there is an authentication that the original encryption could not have been done by any body other than the holder of the private key of the purported sender.

Thus the system of "Private Key Encryption of the hash Value" ensures both authentication and data integrity of the message. This is defined as "Affixing a Digital Signature to an Electronic document".

Taking the earlier example, we had an electronic file represented by the sentence –

> Here is an example of how a Hash Function operates.

Hash code for the above sentence using MD5 is

> a62970c3bfe16618ad6b447b7eae6cc0

When this is encrypted with a PKI system using a specific key, it would look as follows:

> 01c0c5f14dee0d8cbc9ea54c07e296fd01c5ce2dac42387654d
> 69ac63f52fa06
>
> (P.S: The cipher text would be different for different keys)

Now if one applies a given public key (say Naavi's public key) to the above encrypted message and obtains the hash code mentioned above, then it is legally presumed that the file represented by the hash code was originated by Naavi.

If one has an access to the purported original file that contains the sentence "Here is an example of how a Hash Function operates.",

and independently computes its hash code using MD5 algorithm and finds out that it is same as the decrypted hash code, it can be presumed that the document can not only be attributed to Naavi but also confirmed that there were no alterations after his authentication.

This completes the Digital Signature process for authenticating the file in a manner that it cannot be repudiated by Naavi.

In actual practice, affixing of digital signatures as well as their verification are done automatically by the applications which are PKI enabled using the keys that are made available in the user's system.

In case it is necessary to maintain confidentiality of the message, it can be encrypted using either the private key of the sender or the public key of the recipient.

Since the public keys by definition are available in the public domain, no worthwhile confidentiality can be achieved by encrypting any document with a private key. Hence where confidentiality is to be ensured, the body of the document is encrypted using the public key of the intended recipient so that it cannot be opened without the private key of the intended person.

If the document is to be preserved for self use at a later time, it can be encrypted with either a symmetric key system or with the public key of the originator so that it can be opened only with his private key.

NEED FOR A TRUSTED INTERMEDIARY

There are two critical factors in this "Digital Signing" process. They are,

1. Transmission of the public key in such a manner that the recipient is certain that no body other than the purported sender could have sent it

2. Use of a "Standard Cryptographic System" that is acceptable to the legal system.

The Legal system therefore recognizes a role for a trusted third party who would issue a "Certificate" to the sender which can be used as a document that identifies him and his public key to the other contracting parties to whom the digitally signed document is sent.

The certificate would contain the public key of the sender digitally encrypted with the private key of the Certifier himself.

Such a certificate is called the "Digital certificate".

The verification of the certifier's public key is done by a recognized government agency such as the "Controller of Certification Authorities" or through his subordinate certifying authorities and held for public verification in a repository.

The "Root Certifying Authority" would be the ultimate administrative authority for certification having jurisdiction over the process. His identity is like the signature of the Governor of Reserve Bank on the currency notes, accepted widely and verifiable if required.

Thus a unique technological system of encryption and decryption is used to define and implement signatures in the digital society that binds the signatory to the legal consequences of the document.

ITA-2000 has prescribed that the acceptable form of authentication of an electronic document is through affixing of a Digital Signature using "Asymmetric Crypto System" and "One way Hash Algorithm" with the Digital Certificate issued by a "Certifying Authority" licensed by the "Controller of Certifying Authorities". The "Licensing System for Certifying Authorities" ensures the use of approved standard cryptographic and hash algorithms and other procedures for administration of the system.

The popular mail softwares such as the Netscape Messenger or Outlook Express are pre-programmed to recognize the public keys of established certifying authorities so that the browser can accept the public keys of the subscribers contained in a certificate issued by them.

However, the "Root Authority" recognized by the application may not be the same as the "Root Authority" recognized by the Legal system in the jurisdiction of the Certificate user. Hence a certificate issued by Verisign may work perfectly on the Outlook express while a certificate issued by TCS may generate "Chain of Issuing Authority Not Authenticated" or similar alerts even though TCS Certificate may be a legally valid certificate in India while Verisign's certificate may not be so.

In order that the applications recognize the public key of the Certifying authority, they need to be embedded into the application at the OEM level or through specific installation.

ALTERNATIVE ENCRYPTION SYSTEMS

In India the legal position is clear that only a digital signature supported by PKI technology where the digital certificate is issued by an Indian Licensed Certifying Authority is valid.

There is however an yet to be resolved conflict between ITA-2000 which prescribes the minimum encryption standards for digital signatures and the ISP (Internet Service Provider) guidelines which restricts the transmission of encrypted messages above a certain strength.

It is however necessary for us to recognize that many of the secure message transmission systems world over operate on a combination of symmetric and asymmetric crypto systems and with the use of encryption keys in the range of 1024 bits. There are also systems such as PGP (Pretty Good Privacy) which operate on PKI technology and is used by many service providers on the Internet.

The current laws in India make these systems vulnerable to being challenged as legally unacceptable by the courts of law. While this legal validity issue can be sorted out only by a change in the law and cross certification of foreign certifying authorities, we can try to understand how these systems actually function.

SYMMETRIC-ASYMMETRIC COMBINATIONS

When a Netizen visits a "Secure" website where the Server has a Digital Certificate, the data exchange between the Netizen's browser and the server can take place with encryption so that any eavesdropper would not be able to steal the data. In such HTTP transactions, if every packet coming in and going out are to be

encrypted with PKI system, the browsing speed may go down to impractical levels. Also, Netizens who may not have digital certificates may not be able to use the secure mode of transactions.

An alternative system is therefore used for secure transmission of messages during a browsing session.

Under this system, the server which is equipped with a digital signature of its own sends its public key to the Browser as soon as the connection is established. The Browser can then generate a random symmetric key at its end and sends the copy of the key to the server duly encrypted with the public key of the server.

After this secured exchange of the "Symmetric Key", further transactions can take place with the use of the symmetric key alone. The symmetric key issued in such cases will be randomly generated for each session and every new session will use a new session key.

This system is used in secured transaction systems such as SSL (Secured Socket Layer) and HTTPS (Secured HTTP).

SPLIT KEY TRANSACTIONS

There are also some other novel systems developed by some vendors for secure transmission of electronic documents. One such system is a "Split Key Architecture" for secured transmission of data which works as follows.

During the registration process, for the service, a PKI key pair (public and private key) is generated on the sender's machine. The public key and the sender's ID are sent to service provider

(Surety). The private key never leaves the sender's computer.

When the sender composes a secure email message, a symmetric key is generated and used to encrypt the email message together with the sender's digital signature.

This symmetric key is encrypted with recipient's public key and cryptographically split into two secured pieces. One half of the symmetric key is sent to Surety and the other half is sent to the recipient along with the encrypted message.

The recipient receives the encrypted message and half key. To read the message, the recipient must retrieve the other half of the symmetric key from Surety. The halves of the symmetric key are combined and unlocked by the recipient's private key.

The symmetric key is used to decrypt the email and in the final step, the sender's digital signature is validated.

TIME STAMPING OF A DOCUMENT

Digital Time Stamping is another important activity involving security of Electronic Documents. Here, a document is required to be stamped in such a way that the time of creation of the document is recorded and any changes made there in later are tracked.

The normal procedure for such stamping is that the party requiring the stamping creates a "Digital Signature" of the document under the PKI system and sends the digital signature/encrypted hash to the service provider. The service provider records the receipt and returns the digital signature enveloping it in a certificate that also certifies the time of receipt and the originator.

This service has enormous value in preserving the evidentiary value of electronic documents.

TWO KEY PAIR SYSTEM

The need of the Netizens to exchange confidential messages with good encryption does some time have conflict with the needs of the regulators to have access to the communication for monitoring purposes.

As a result, if the authorities get hold of a communication which is encrypted with the public key of a Netizen, they would need the corresponding private key to decrypt the message. Otherwise they need to crack the key by force.

If the private key is held by an individual who can be traced, arrested and compelled to part with the key, the decryption would be facilitated. In case the holder of the private key is not traceable or is non cooperative or has genuinely lost the private key, the decryption of the message becomes impossible.

In order to deal with such situation, a suggestion has been made that the Digital Signature system has to be designed with a dual key pair. One key pair for the purpose of encryption of the document and the other for the digital signature.

In such a system, it is proposed that the set of keys meant for the signature purpose is generated in the user's computer and the corresponding private key held in total control of the user. The CA will get only the public key which he wraps in a certificate and returns.

On the other hand, the other set of keys meant for encryption

may be generated at the CA's end and CA would hold the copy of the private key meant for encryption.

In the event of an emergency, the authorities can take a copy of the private key of an individual from the CA and decrypt the incoming messages of a Netizen either confidentially or otherwise.

In India the first CA to be licensed, namely Safescrypt has not enabled the issue of dual key pairs. However IDRBT (Institute for Development and Research in Banking Technology, promoted by RBI) which has also been licensed as a CA is enabling their system for the dual key pair use.

These are however compatible only with the new versions of the e-mail clients such as Internet Explorer or Netscape Messenger and others may need to use a special plug-in to use the digital certificates to be issued by IDRBT.

CHAPTER V

DIGITAL IDENTITY MANAGEMENT

The backbone of the legal system in the digital society is the ability to recognize digital signatures. ITA-2000 relies on the "Asymmetric Cryptosystem" where the originator of the document generates a key pair and forwards the public key to the addressee.

When a person receives a public key ostensibly belonging to a person named therein as the originator of the key, he needs to verify the correctness of this claim. This process of verification is done by the use of an intermediary who has the trust of both the parties. The originator can hand over the public key to the intermediary and he can deliver it to the addressee. For this system to work on the virtual world, even this intermediary should be digitally recognizable by both the parties.

CERTIFYING AUTHORITY

This mediatory role has been assigned in the legal system to approved "Certifying Authorities" (CA). These CA s are registered with the ultimate body which controls the digital signature system. Their own public keys are certified by such "Root Authority" directly or through a chain of other registered certifying authorities each identifying the public key of his predecessor in the chain of certifying authorities.

In the Indian law the root authority would be the "Controller" of Certifying authorities who may appoint "Deputy" and "Assistant" Controllers to assist him.

The Controller will also be the "Repository" to hold all Digital Signature Certificates issued under the proposed act and also a list of "Revoked" Certificates.

DIGITAL CERTIFICATE

Digital identity in the case of Internet transactions is required by the individuals who send e-mails, as well as by "Servers" who act on behalf of one of the contractual parties as an "Electronic Agent".

Thus there is a need for Individual's Digital Certificate and a Server's Digital Certificate.

The CA s would take an application from the persons who intend to sign electronic documents and issue "Digital Certificate"s to them.

In the first step of such an issue, the CA would verify and confirm the particulars about the applicant which is required to be incorporated in the Digital Certificate by mapping the identity of the applicant to a physical identity document such as say the individual's Passport or a Company's registration certificate.

After being satisfied with this identity process, the Certification issue process would commence.

When this request for Digital Certificate is being processed between the user's computer and the CA's Certification server in a "Certificate Issue session", the user's browser would generate the key pair using a software approved by the CA. The private key is stored in the computer and would be available whenever a document is to be signed. The public key is sent to the certifying

authority to be embedded in the Digital Certificate issued by the CA.

The certificate duly incorporating the public key of the subscriber and any other details such as his name and e-mail address is returned to the subscriber.

This entire process of "Random Generation of Key pair", sending of the public key to the CA and its return as a Digital Certificate takes place in one single session when the applicant's computer is connected with the CA's Certificate issuing server.

A typical Digital Certificate issued to an individual looks as indicated in the picture at the end of this chapter.

If during the process of Digital Certificate issue, the session is interrupted, the process of key generation would be repeated again in the next session. It may be noted that during the entire process of the Digital Certificate issue, the private key never leaves the computer of the Certificate applicant. Only the public key traverses to the Certifying Authority's end and comes back in the form of a Digital Certificate.

Every certificate is an electronic file that includes information such as the name and email address of the certificate holder, an encryption key that can be used to verify the digital signature of the holder, the name of the company issuing the certificate and the period during which the certificate is valid.

Once the subscriber confirms his intention to publish the certificate, it is placed in a repository maintained by the certifying authority himself or any other authorized agency.

The user of the certificate would send it to his addressee whenever he needs to send a digitally signed document. The recipient of a message can also retrieve the certificate from the repository. Such a search can be initiated by the browser or e-mail client automatically.

These certificates can be used as online identification, much in the same way a driver's license can verify your identity in the physical world.

Certifying authorities gather adequate information about the applicant person or company before issuing the certificates. Some Digital Certificates are issued only after the applicant presents himself before a representative of the CA and presents his identification documents. Depending on the type of verification used, the Digital Certificates are classified as "Class A", "Class B" etc.

Some of the CA s also assume liability against losses arising to third parties out of such issue of digital certificates and hence take all the necessary and sufficient care in the process. Such liability limits are called "Reliance Limits". None of the Indian CAs have presently proposed a "Reliance Limit" for their certificates. Contents of Digital Certificate

According to Certifying Authorities Rules under the ITA-2000, all Digital Signature Certificates should *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.

Certifying authorities may develop their own systems and classes of certificates that provides different degrees of assurance on the identity of the certified user of the digital certificate.

In the Indian context the "Controller" prescribes the minimum required levels of assurance as a part of the rules to be formed in this regard. The standards concerning the digital signatures as indicated in the rules are as per the following table.

Standards Prescribed by ITA-2000

The Product	The Standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
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

RSA Public Key Technology..contd	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

CERTIFICATION PRACTICE DOCUMENT

The Certifying Authority (CA) is expected to follow prudent systems and practices to verify the information provided by the applicant when he applies for a certificate. Such practices would be contained in a public document called "Certification Practice Document" which will be made available for public knowledge through the repository.

A CA is also expected to use trustworthy systems to generate and manage the Key records and to approve only such systems to be used at the subscriber's end that would not put the system under undue risk.

The CA is expected to cause the revocations and expiry of certificates to be duly noted in the repository as a "Certification Revocation List" so that any user can verify the validity of the certificates.

According to the licensing procedure for CA s prescribed under the ITA-2000, a Certification Practice Statement has to accompany the application for license and should be acceptable to the licensing authority.

It must be noted that Section 35 of the ITA-2000 when the Act was passed contain a drafting error noting that the Certification practice statement was a mandatory document to be submitted by every applicant for a digital certificate to the CA. [Section 35 (3)]. This has since been corrected through an administrative notification.

REGISTERING AUTHORITIES

While the issue of Digital certificate is a technology intensive activity, the need to identify an applicant and verify documents of identity such as a passport or a driving license or a ration card or an Income Tax PAN card etc is an activity which requires presence near the markets.

In order to accomplish the identification job, many CA s prefer to use an intermediary service provider called the "Registering Authority" (RA). The applicant to a Digital Certificate is normally required to meet the RA after making a provisional application to the CA along with the identification documents prescribed for the issue of the certificate as per the certification practice statement. The RA receives the copies of documents presented, verifies and certifies to the CA that the same are in order. He also keeps proper documentation for the purpose.

The certificate would be issued by the CA only after the input from the RA is obtained.

Some times CA s may not appoint formal RA s but accept the services of public servants such as the Bank Managers, or Chamber of Commerce officials etc for such identification.

The ITA-2000 has not dealt with the requirement of an RA in the digital certification system. Considering the importance of RA s in the identification and therefore on the non repudiation character of a digital certificate, it would have been necessary to recognize their role in the Act itself. However the Act is silent on the subject and leaves the inter-se responsibilities between the RA and the CA to be determined through the contract of agency.

CROSS CERTIFICATION

Another grey area left by the ITA-2000 regarding the activities of CA s is the process of Cross certification.

Essentially, "Cross Certification" means the automatic authentication of Digital Certificates issued by one CA by another.

For example when multiple CA s are functioning in the country, a person may obtain a certificate from only one such CA. Suppose he wants to use it for signing a digital contract, the other contracting party may be in a different country and may not feel comfortable with the CA who has issued the certificate. He may have faith in a CA who is operating in his own country. In such a circumstance, it would become necessary for the two CAs to develop a system of cross-certification amongst them so that the users can proceed as if the Certificate was issued by their own trusted CA.

Such Cross certification therefore becomes necessary when the contracting parties are from different jurisdictions.

According to ITA-2000, while there is a provision for a foreign certifying authority to be licensed through an appropriate procedure, it requires an application by such a certifying authority.

In the absence of such application and approval, any Digital certificate issued by a CA who is not licensed by the Controller in India becomes invalid.

There is therefore a necessity for cross certification of an international CA by a local licensed CA. This has been provided for under the Information Technology (Certifying Authority) Rules 2000, (rule no 12).

The same rule also prescribes that cross certification between different CA s licensed in India is mandatory and such an arrangement should be submitted to the Controller before the commencement of the operations. Since all the CA s licensed by the controller would be within the legal jurisdiction of Indian judiciary, this mandatory need seems to serve no practical utility but imposes an unnecessary burden on a CA applicant to approach his business competitors for cross certification.

The rule is ambiguous as to whether the CA who is licensed first needs to grant cross certification to the new CA for his "To be issued Certificates" or it is only obligatory for the new CA to agree to accept the validity of certificates already issued by the earlier CA.

Perhaps this rule is meant to achieve a "Technology Compatibility" of digital certificate systems so that certificates issued by different CA s can be cross platform compatible.

VALIDITY OF DIGITAL CERTIFICATES

A Digital Certificate is issued for a specified validity period as per the Certification policy followed by the CA.

The CA may revoke the certificate under the following circumstances:

- On subscriber's request
- On the insolvency or death of the subscriber
- Where the subscriber is a Firm or Company, upon their dissolution.
- If any material fact provided by the subscriber is found to be false or a requirement found not complied with,
- The private key of the CA or his security system is compromised.

The CA may suspend the certificate under the following circumstances:

- On receipt of request from a person whom the CA has reasons to believe to be the subscriber or his authorized agent.
- If the CA considers it necessary in the public interest.

In such cases of suspension the subscriber should be given an opportunity to be heard in the matter within 15 days.

FINANCIAL LIABILITY OF THE CA

The Certifying authority would normally be financially liable to third parties in case of any loss they may suffer on account of the

negligence of the CA in issuing the Certificate or allowing its usage.

He may, if he so desires specify a recommended "Reliance limit" in the certificate up to which his liability may extend.

Normally, the CA would not be liable for any losses caused by reliance on a false or a forged digital signature of the subscriber in case he has complied with all the necessary precautions/procedures envisaged in the proposed act.

Also, his liability would be limited to the reliance limit specified if any, even for a loss caused by misrepresentation of facts by the subscriber or by the CA s own failure.

The existence of such a reliance limit on a certificate is a matter to be specified in the Certification practice Statement. None of the Indian CAs at present have proposed reliance limits for their certificates.

CUSTODY OF THE PRIVATE KEY

Once the subscriber accepts a certificate, he is duty bound to exercise reasonable care in the custody of the private key so that its confidentiality is not compromised. The key is stored in the hard disk of the user's computer and if the computer is shared with some body else or if the computer is stolen, it may become available to others.

The key is expected to be stored in a password-protected file so that even if some body has an access to the computer occasionally they don't have access to the key.

It is needless to reiterate that the password to the Key file itself needs to be protected from being compromised.

Users should remember that unlike other passwords that they use in the computers to gain access to a web site or see their mails, the password to the digital certificate file needs a far higher level of security. It is like holding a fully signed blank cheque book and has to be held in sole personal custody. Noting down the password in a manner available to others should be strictly avoided.

Whenever a private key is lost or its confidentiality is compromised, the subscriber is expected to inform the CA so that the certificate can be revoked. If this is not done, any body in possession of the private key of the subscriber can proceed to use it fraudulently to sign electronic documents on behalf of the original holder of the key.

ITA-2000 makes it an offence for a digital certificate applicant to provide incorrect information to the CA at the time of application or using a Digital Certificate for fraudulent purpose punishable with imprisonment up to two years and/or a fine of up to Rs one lakh.

CERTIFICATION REVOCATION LIST

Every certifying authority therefore maintains a real time Certification Revocation List (CRL) which can be verified before any certificate is to be relied on.

Computer users who do not understand the full import of managing password security, and executives who instinctively operate only through their secretaries would better not rush into obtaining digital certificates as the consequences of Key misuse

could be disastrous.

Similarly, a corporate entity, which may like to obtain digital certificates for its employees to enable e-commerce transactions, will have to selectively authorize people with the right credentials to offer digital certificates on behalf of the company.

CORPORATE ENVIRONMENT

In the Indian corporate environment, persons who may operate the digital certificates on behalf of the company may have to be authorized through a board resolution. Even though this may not alter the liabilities of third parties contracting with the company on the strength of the digital certificate, it may determine the rights of the Signatory or the Board of Directors vis-à-vis the Shareholders.

Companies will also need to develop a proper system for retrieval of encrypted archived documents in case the vault manager who archived the files is no longer available.

Shared Computer environment and configuration of firewalls to delete attachments are incompatible with the Digital Signature usage and must be avoided.

SECURED CUSTODY OF ELECTRONIC RECORDS

Normally electronic documents are stored in removable storage devices or computer systems behind a firewall (A hardware and or software device that restricts entry to a protected system based on a preset authentication procedure). The emerging practice is to store data at least temporarily in a virtual back up server.

While removable storage devices can be locked away in a physical vault, the data stored on a computer system either within the owner's premises or elsewhere needs to be kept safe from a hacker.

In such cases, it would be preferable to store the document in an encrypted form. When the document is so stored in an encrypted manner, it becomes necessary to preserve the decryption key of the "Document Custodian" so that the documents can be restored on a future date in his absence by the relevant authority in the organization.

Will the CIO hold the Key?

ITA-2000 prescribes the methodology for authentication of Electronic documents through the combined use of a "Hash Algorithm" and "Asymmetric Cryptography".

This Digital Signature process relies on the ability of the signatory to keep the private key solely under his custody. Since the private key is a file that is stored in the computer of the user in a password protected file, the integrity of the private key in turn depends on the ability of its owner to control this password.

This control process starts from the moment one applies for a digital certificate and with the generation of the key pair itself. The standard procedure of digital certification goes through the following steps.

- The Certifying Authority receives an application for issue of a digital certificate with the prescribed information.

- The Certifying authority verifies the information as per his certification practice policy and satisfies himself about the identity of the applicant. In some cases, he may only verify the authenticity of the e-mail address. In some cases he may verify identity documents such as the Social Security card, passport or the IT identification card (PAN card). In some other cases, he may even meet the applicant in person through an authorized representative and establish the identity through a "Notarization like" process.

- When the Certifying authority is ready to issue the certificate, the applicant is invited for an interactive session with the certification software. During this session, the

software will generate a pair of Private and Public Keys within the applicant's computer. During the process itself, the private key is tucked away in a password protected file within the applicant's computer and the public key alone is sent to the certifying authority for certification. At the Certifying authority's end, the public key will be received and put into a file containing other particulars such as the name and address of the applicant, expiry date of the certificate etc and encrypted with the private key of the Certifying authority. This encrypted file is the "Digital Certificate" that is sent back to the applicant.

- The applicant can then distribute it to the persons to whom he intends sending his signed communication. The Certifying authority will also place it in a repository where the message recipients can search and retrieve it if required.

This entire session has to be managed by the applicant successfully to get a Digital Certificate.

Subsequently the password to the protected file containing the private key has to be operated by the signatory as if it is an approved facsimile signature stamp which needs to be protected at all times. For continued safety, the password should be well constructed to prevent breaking by a

criminal inside or outside the organization. If the CEO has the habit of using his wife's, Children's or Pet Dog's name as password, it will be a cakewalk for an insider to generate any electronic message that may bind the CEO legally.

At the same time the CEO should not store the password in a chit or in his diary. He should also keep changing the password frequently but not forget it.

He should also ensure that his Computer is never shared even with his colleagues.

In the corporate environment, we often find that the CEO or the Functional executives are often not Computer savvy. They often manage their e-mails with the assistance of their secretaries. Such executives may

find it difficult to go through the process of digital certificate generation and control of private key all by themselves.

Unfortunately, this is one activity where no assistance can be taken by the executive without the danger of his signature being forged.

It is this responsibility that calls for a separate hierarchy for bestowing digital signing powers in an organization. For example, if the CEO or the functional managers are not comfortable or capable of handling the private keys to their Digital certificates, they may rather keep themselves out of Digital signing hierarchy. If need be, they can send a conventional written authentication to the designated "E-Transactions Controller" who in turn would affix his Digital Signature before the electronic version of the document is sent out to a recipient.

It may therefore be the privilege of the CIO to hold the vital "Key" to the digital communication of the company and rule the E-Commerce world of the company as a proxy of the CEO.

CHAPTER VI

BUSINESS OF CERTIFYING AUTHORITIES

Certifying Authorities are the agencies who issue digital certificates to individuals or computer systems and have a vital role to play in the administration of the Cyber Laws.

Certifying Authorities (CAs) are the authorities who create a distinct identity to the contracting parties in the digital world. They provide the confidentiality to the transactions that enhance the confidence on the digital media with the users.

They provide the non-repudiation assurance, which is the backbone of digital contracts. They also enable encryption of documents so that the contracting parties are assured of non-tampering of the documents.

THE REQUIREMENTS OF A CERTIFYING AUTHORITY

The responsibilities to be borne by the Certifying Authorities are onerous. They need to use sophisticated software to generate encryption that cannot be broken into. They need to hold the Registry of keys and the Certificate Revocation List away from hacker attacks and updated on real time basis.

They need to employ staff with the necessary expertise and also the necessary integrity to keep the trust of the community. In the event of any certificate being misused, CA s also may have to provide financial compensation to the affected parties.

In some countries like India, there is a "Licensing System" and only licensed authorities can issue legally valid Digital Certificates. In some countries, certain standards are given by the authorities as guidance to the market and the Contracting parties are free to use the services of Certifying Authorities of their choice.

According to the Information Technology Act, the Controller obtains applications from aspiring Certifying Authorities and issues licenses. The necessary rules have been notified indicating the capital adequacy, the eligibility criteria, the security norms etc.

Considering the possible financial liability, financial soundness is an important criterion in approving a certifying Authority. However, the capability of a CA to keep itself always at the very top of the technology developments cannot be underestimated. The "Ability to prevent a liability from arising" should therefore weigh more than the "Financial muscle to meet the liability" when it arises.

Having said this, it should also be remembered that many of the technology wizards in the world are potential hackers for fun, gain, revenge, or otherwise. The power of technology that an intelligent young software wiz kid controls could easily intoxicate him in to turning anti social at the slightest pretext. To hold such potential mine fields and manage a trusted organization would be one of the most challenging tasks for the management of the Certifying Authorities.

An ideal Certifying Authority should therefore possess impeccable integrity at all levels in the organization and outstanding technical and managerial skills. Additionally they need appropriate marketing skills to sell the new concept to a virgin market.

It is not surprising therefore that it has taken nearly three years since the passage of the ITA-2000 for two CAs to emerge in India who can issue Certificates to the public and even they are yet to fully appreciate and fulfill their role responsibilities to the market

LICENSING GUIDELINES

The principle guidelines prescribed by the Controller of Certifying Authorities for licensing CAs in India are as follows:

Eligibility:

The persons eligible for applying for a license as a Certifying authority in India are:

a) An Individual, being a citizen of India and having a capital of Rs 5 crores or more in his business or profession
b) A Company having a paid up capital of not less than RS 5 crores and a net worth of not less than Rs 50 crores with a non resident and foreign holding not exceeding 49 %. (In the case of a newly formed company exclusively to carry on the business of CA, the net worth will be computed as the aggregate of the net worth of the Indian promoters)
c) A firm having a capital subscribed by all partners of not less than Rs 5 crores and foreign holding not in excess of 49 %. (In the case of a newly constituted partnership exclusively to carry on the business of CA, the net worth will be computed as the aggregate of the net worth of the Indian partners.)
d) Central Government or State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Location

The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as the maintenance of the directories containing information about the status and validity of Digital Signature Certificates shall be installed at any location in India.

License Period

The CA license is being presently issued for a 5 years and is non transferable.

Security Guidelines

The CA s have to adhere to the detailed guidelines issued by the Controller regarding Security of the systems as well as periodical audit etc.

INDIAN CERTIFYING AUTHORITIES

The first Certifying Authority to be licensed in India was Safescrypt (http://www.safescrypt.com) which is a joint venture between Satyam Infoway (SIFY) and **Verisign**. It started operations in February 2002 and presently offers Digital Certificates to Indian public.

Subsequently, IDRBT, (Institute for Development and Research in Banking Technology), a subsidiary of the Reserve Bank of India obtained its license as CA. It is presently issuing Digital Certificates only for Bankers to enable inter bank fund transfer.

TCS (Tata Consultancy Services) became the third CA to be licensed in India and offers its services to public through its website http://www.tcs-ca.tcs.co.in

The fourth CA to be licensed in NIC (National Informatics Center), the Government of India enterprise which is expected to cater to the requirements of the Government sector.

OPPORTUNITIES FOR INTERNATIONAL PLAYERS

ITA-2000 has provided that the Controller of Certifying Authorities may with the previous approval of the Government recognize any certifying authority operating outside India to issue digital certificates under the act.

However, according the rules currently in force, licenses for Certifying authorities would be issued only if the facilities for issue of the Certificates exist in India. Hence it would be necessary for a foreign Certifying authority desirous of getting licensed in India to set up the facilities in India.

Some of the leading certifying authorities in the International arena include Verisign, Thawte, Global sign, etc. In addition to dedicated Certifying agencies, some ISP s and Banks abroad such as British Telecom and Scotia Bank are also into this business. Verisign which also owns Thawte is the market leader and is already in the Indian market through Safescrypt.

SERVICES OFFERED

The certifying agencies typically offer personal identity certificates to individuals as well as secured server identifications for computer systems. They also provide "Managed Services" where a

company can issue certificates for all its in house requirements using the technology provided by the CA.

PERSONAL E-MAIL IDENTITY CERTIFICATION

With a personal e-mail ID, a subscriber can send his/her emails with an attached signature file created with his private key. This Signature can be read with the corresponding public key embedded in the digital certificate.

There are different classes of such personal digital certificates that are being used at present. At the first level, a certificate only certifies the e-mail address without the name of the person being associated with it.

At the second level, the name is added to the certificate without physical verification. More trusted certificates make it mandatory for the subscriber to physically present himself before a person or organization trusted by the certifying authority who can verify some personal identification documents and authenticate the identity. This notary like service creates a bridge between the virtual world and the physical world and makes the identification process a highly reliable mechanism.

The financial limits up to which the certifying authority guarantees the certificate usage associated with these different classes of Certificates vary and so are the charges for the service.

SECURED SERVER CERTIFICATION

Most of the transactions on the Internet are concluded on or through a web server and just as an individual needs a certified identity, even the web hosts need a certified identity. Otherwise, a

mischievous operator can set up a site only to collect credit card and other personal details for the purpose of defrauding the Netizens. Hence the certifying agencies provide a server certification facility as well.

Similarly, companies running virtual private networks connecting their employees over a public network and financial institutions such as Banks also need certifications that enable the servers to communicate with the network clients in a secured manner and manage in house certification systems. Some of the certifying agencies provide such value added certification services.

The Dilemma of the Digital Signer

The proverb, "An Early Bird Catches the Worm" is well known. But it is also true that from a different perspective one can rewrite the proverb and say "The Early Worm Gets Caught". The dilemma of the early adapters to the Digital Signature regime is similar. Presently, if an e-mail communication is sent to an Indian using the Digital Certificate issued by a licensed Indian CA, then the e-mail will have total evidentiary value. In other words, the recipient of the mail can produce the digitally signed e-mail as an irrefutable evidence against the sender.

However, if the sender has to use it as an evidence against the addressee, merely producing his own digitally signed e-mail from his "e-mail sent box" will be of no value. What is required is either a specific acknowledgement from the receiver or any action that can be used as an evidence of such receipt.

According to Section 12 of the ITA-2000,

Where

the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method,

an acknowledgment 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*

Further, Where

the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him,

then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Also Where

the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment,
and
the acknowledgment has not been 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 acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment 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.

According to the above provisions, for the purpose of creating a valid acknowledgement, even an automated response or some action that can be linked to the fact of receiving of the message is a necessary and sufficient condition to constitute a receipt.

It is therefore essential to understand that any sender of a digitally signed e-mail has to protect his interest by extracting an acknowledgement from the recipient without which he will have no evidence for having dispatched a message to the addressee.

Since any extraction of acknowledgement by the sender of the mail would be a self serving evidence in case of a dispute against the addressee, it is better if a third party is involved in witnessing the transaction. One of the ways by which this condition can be fulfilled is with a third party witnessing the dispatch of the mail as described in the proposed Cyber Evidence Archival Center. (http://www.ceac4india.com).

Another problem that a digital signatory would come across is when the addressee uses a digital certificate issued by a CA who is not licensed in India and who is not carrying a Cross Certification with an Indian CA.

Here also, the evidentiary value of the digital signature of the addressee is likely to be rejected by the Indian Courts despite this being to the disadvantage of the sender using the Digital Certificate of the Indian CA. Here again, a service of Cyber Evidence Archival could come in handy.

Thus despite the technological marvel that the Digital Signature system is and its proven utility for preserving data integrity and authentication, there are certain practical problems in building an exchange of digital communication into a valid digital contract using digital signatures and these have to be borne in mind by the Digital Contract enthusiasts. Alternatively, Cyber Evidence Archival services should develop as complimentary services to Digital Signature services.

CHAPTER VII

DIGITAL CONTRACTS

A contract is essentially an agreement enforceable in law. It consists of an offer from the originating party and an acceptance from the other party to the contract. Electronic Contracts are contracts where the offer and acceptance are exchanged through electronic documents. There may also be semi electronic contracts where part of the offer and or the acceptance is conveyed electronically while the rest is conveyed through the conventional system.

Even though the Information Technology Act-2000 has not dealt with Electronic contracts in specific detail, by virtue of Sections 3 and 4 of ITA-2000, we can conclude that the provisions of the Indian Contract Act should be applicable even to electronic contracts.

We may therefore proceed with the presumption that except where for any mention has been made to the contrary, electronic contracts are governed by the provisions of the Indian Contract Act with the words "Electronic Record" and "Digital Signature" replacing the terms " Written document" and "Signature" wherever they appear.

CONTRACTS THROUGH ELECTRONIC AGENTS

ITA-2000 has indicated in Section 11, to whom an "Electronic Record" can be attributed.

It states as follows:

> 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.

In the digital world, it is common for automated systems to respond to standardized queries. Keeping this in mind ITA-2000 has recognized contracts formed by the interaction of an electronic agent and an individual through this section.

Thus Section 11 (C) makes it possible for the existence of "Electronic Agents" where as the Indian Contract Act recognizes only "human agents". Just as the Indian Companies Act makes it possible for the existence of a "Corporate Person" as a legal entity, we can therefore say that ITA-2000 has recognized the existence of a "Digital Person" who can act as an Agent and to whom documents can be attributed.

We may note that any electronic record generated by an information system programmed by or on behalf of the originator to operate automatically, will be attributed to such an originator. Here the term "Originator" refers to the programmer or to the person who appointed the programmer to develop such a programme.

It may be considered that for the clause "On behalf of the originator" to become operative, it would be necessary that the said automated function should be specifically authorized by the owner. In case no such instructions have been given and the "Programmer" has not kept the person who appointed him appropriately informed about the functions of the software, the

responsibility for any electronic document generated by the automated system may have to be borne by the programmer.

CONTRACTUAL ABILITY

In the paper world, a valid contract also requires that the signatories are not minors or insolvent persons and are of sound mind at the time of entering into the contract. Contract should also not be under Misrepresentation, Fraud, Coercion and Undue Influence or under any mistake of fact and for unlawful purpose or consideration.

All these principles may apply to Digital Contracts also.

Out of these conditions that are required to be fulfilled for any Contract to be valid it is interesting to note that "Undue Influence" is presumed in certain cases of relationships in the real world such as between the "Doctor" and the "Patient", "Lawyer" and his "Client" , "Husband" and "Wife", "Father" and "Child", "Employer" and "Employee" etc.

In future, such presumptions may also be extended between a "Computer Programmer" and his "Programme" or the buyer of the programme.

ELECTRONIC DOCUMENTS AS WEB PAGES

ITA-2000 has not specifically discussed the status of documents appearing on web sites. However, the definition of an "Electronic Document" will include the web page.

Also, while defining Cyber Crimes, the Act does recognize some of the rights of the Web site owners.

It is presumed that the site owner has reasonable control over what is published on the site. It is also possible to fix the identity of the owner of the web site who has to be presumed as the originator of the Web document unless otherwise specified.

Even though, the document may not be signed individually, if the site is in a public domain, it is possible to produce circumstantial evidence to prove that certain content existed on the site at a certain point of time. The web page may therefore be considered as an open offer from the site owner if the contents therein imply such an intention.

When a Netizen enters a web site, he makes a request for an electronic file to which the web server responds. It is like asking for the open contract offer from the web server. If the visitor submits any response based on the offer available on the web page it may be possible to argue that a contract has been completed.

The contract through the web interface in an unsecured web site cannot automatically qualify as an exchange of digitally signed documents.

But, in a secured site with restricted entry, the visitor identifies himself before accessing the site. Any action taken by the Netizen under such circumstances while on the site is therefore between two identifiable parties. If the visitor has also derived a benefit from his visit such as receipt of a product, which he has agreed to purchase, there is clear evidence as to the intention of the web interaction.

In view of the above consideration, even without a specific exchange of digital signature, a web interface where an offer and

acceptance is exchanged, may also qualify as a valid contract. Perhaps they could be equated with oral contracts which are also valid in law, but may need the support of circumstantial evidences to prove.

It is this fact which should keep an ordinary Netizen alert to the implications of the Cyber Laws.

DIGITAL CERTIFICATES AS ENTRY PASSES

There are web sites that provide an entry based on a digital certificate. If a visitor offers the certificate for gaining his access, he may be completing a signature process that may have implications while he is on the site.

TIME AND PLACE OF CONTRACT

Yet another important aspect of Electronic Contract process is to determine the time and place of creation and the time and place of delivery of the documents so as to determine the commencement or end of a liability arising out of the contract.

As per the provisions of the ITA-2000, the despatch of an electronic record occurs when it leaves the system of the originator and enters an information system outside his control unless otherwise agreed to between the parties. (Section 13)

The time of receipt of the document at the addressee's end would depend on the mode of receipt of the document used by the receiver.

If the recipient has designated an information system for the purpose of receiving electronic records, receipt occurs when the

record enters such system.

If the electronic record has been sent to an information system not designated by the addressee, the receipt is deemed to occur at the time he retrieves the information.

If the addressee has not designated any system for receipt of the record, the receipt occurs at the time the record enters the information system of the addressee.

Unless otherwise agreed, an electronic record is deemed to be despatched 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.

These provisions are very important in the context of web related transactions where the web servers and responder systems may be situated in places other than the place where the originator or the addressee may have their businesses.

It is also necessary for the parties entering into digital contracts to specify the e-mail addresses at which they would receive their messages. It is common for people to hold multiple E-mail addresses to be used for different types of transactions. When they enter into contracts, the default e-mail address mentioned in the browser or the mail software may be recorded as the representative e-mail address of the party.

If the person prefers to use a specific e-mail address for a contractual communication, it would therefore be a good practice to include a note at the end of the message indicating his e-mail address to which future communication should be addressed.

JURISDICTION OF CONTRACTS

ITA-2000 is specific about the determination of Time and Place of dispatch of an Electronic Document which can be used to determine where a contract was completed and therefore fix the jurisdiction of the Contract. However, since digital contracts are often struck between parties in different countries, conflicts in law are common.

In many states of USA, the "Customer Contact" is considered a point to determine the jurisdiction. If therefore a businessman is selling his wares in California then he is subject to the jurisdiction of the State laws.

Hence the presence of an office of contact as mentioned on a website through which a contract was entered into could be decisive in certain cases to determine the applicability of local laws.

The case of Yahoo.com being questioned by French authorities for facilitating sale of Nazi memorabilia which is prohibited in France also opened the question of whether jurisdiction should be determined based on the nationality of the contracting party or the place from which he accesses a service.

In one of the recent cases, a Californian court held that since the website owner had the knowledge that a number of his clients were from the State of California and he continued to do business with them, made him accountable to the local laws.

A view to consider is also to take into consideration the mode of making an offer or acceptance. If say a consumer walks into a web shop and concludes a contract, the place where the web shop is deemed to be located which could be the place where the owner is located, should have the primacy of consideration. On the other

hand, if the web shop sends an e-mail message and a contract is concluded by the consumer by clicking an acceptance on the e-mail message, the conclusion would be at the place attributable to the Consumer.

Another area of conflict is in the wordings used in drafting the web contract offer. Depending on the language used, the web offer document can be concluded either as an "Offer" document or as an "invitation to offer" document.

An "Offer Document" completes the contract as soon as the consumer clicks on the "I Agree" button.

In an "Invitation to Offer" document, when the consumer clicks "I Submit" button, he has only accepted an invitation to offer and is making his own offer to be accepted by the web site owner.

These differences have a significant impact on not only the jurisdiction of a contract but also the time of contract and time for retraction from a contractual offer.

To avoid a conflict therefore it is essential that every web contract should clearly specify the jurisdiction so that neither party is in doubt.

Jurisdiction- A Nightmare for E-Business

In all aspects of Business, one which gives nightmares to a Businessman is the factor of "Unknown Risks". In the context of E-Business, Digital Contracts and Transactions over the Internet, what the E-Business entrepreneur dreads most is the Cyber Law related risks which may lurk around the corner and hit him just when he thinks "I have arrived".

For a law compliant individual, who has a workable business model, it is critical that his otherwise viable business is protected from liabilities on account of laws that he is not aware of. There have been many instances when legal action has killed many promising business initiatives.

In normal legal circumstances it is an accepted rule that "Ignorance of Law is Not a Defense". As long as this concept was being implemented within a limited jurisdiction of one country, which is either as small as England or as large as China, there was a reasonable assumption that the Businessman either on his own or with the assistance of professionals could gather enough knowledge of law to steer clear of violations.

E-Business on the other hand is a different proposition. While, from the Marketing point of view, the Businessman is happy that with one website he can reach out the entire globe, he cannot forget that by the same yardstick, he is exposing himself to the legal risks of the entire globe.

The matter of "Jurisdiction" has therefore been of interest to E-Business enterprises.

When ITA-2000 was passed with section 75 of the Act providing extra territorial jurisdiction to bring Cyber Criminals to book, many considered this as an unblemished boon.

The Section states,

> **Sec 75.Act to apply for offence or contraventions 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

This was however a trap in the UNCITRAL model law and exists in the Cyber Law statutes of many other countries. As a result, similar provisions exist in the laws of Malaysia or South Africa and expose Indians to the Global set of laws in all respect. It is not as if this section is relevant only for "Criminals". It extends every aspect of the Cyber Law including formation of digital contracts, conduct of E-Business etc to the global domain.

Countries such as South Africa have been more explicit in their E-Commerce enactments and protect their citizens against E-Businessmen (Including those from outside the Country).

The celebrated dispute between Yahoo and the French Government where the French Government is claiming jurisdiction over Yahoo Website while Yahoo is prepared to admit only a restricted jurisdiction is an important case to take note of.

There have been many other conflicting judgments where the issue of Jurisdiction is looked at differently by different Courts for different types of offences.

For example, in Forrest v. Verizon Communications, Inc., which was a Consumer Protection case, the forum selection clause was upheld for jurisdictional purpose. If this is adopted as a universal principle, then perhaps the E-Businessman and the Customer know what they are contracting.

In Gorman dba Cashbackrealty.com v. Ameritrade Holding Corp. the court held that in the case of an interactive website, the jurisdiction extends to the area of residence of the customer. This could negate the principle of specific forum selection as the basis of determining Jurisdiction.

In Griffis v. Luban, which was a case of Libel, the Court refused to allow extension of jurisdiction.

Under these confusing circumstances, the recent Judgment in the case of Metro-Goldwyn-Mayer Studios, et al. v. Grokster, Ltd., et al in the United States District Court For the Central District of California Western Division has opened a new chapter. This Judgment clearly sets out the rules under which the Californian Courts assume Jurisdictional control over any service which is being used by the Citizens of the State.

According to the judgment,

California authorizes its courts to exercise personal jurisdiction over non-resident defendants to the full extent permitted by the United States Constitution. As such, its courts can exercise jurisdiction over a defendant if he has "certain minimum contacts with the forum [state] such that the maintenance of the suit does

not offend “traditional notions of fair play and substantial justice."

Though in the case in question the extension of jurisdiction was only from the State Jurisdiction to the Federal Jurisdiction, under the principle it established, it is possible that if you have a successful business run from India and have clients in California, then you may have to adhere to the regulations of California.

If this becomes a universally accepted principle, then every Indian E-Business will be subject to the Cyber Laws of every other Country including the many states under USA having different sets of law.

It is therefore an onerous task for any E-Business to hedge against all legal risks that afflict the entity.

While Naavi considers that Cyber Law Compliancy is the essential part of Business and every Portal or E-Business should address this issue without neglect, it is also necessary to debate if a time has come to question this basic concept that "Ignorance of Law is No Defense" since it is unfair to expect any Company to be fully aware of all the laws of all the countries in the world.

Probably, in case of Cross Border disputes of E-Transactions, "Notice of Infringement" must be made mandatory before any action.

While one may argue that the law is same for all and the same law gives the power to an Indian Consumer to file a case against a Pornographic Site in USA, it is obvious that the practical situation is different. No Indian consumer will have enough resources to fight a case in USA and even if it does, as was evident in the Yahoo case there could be different interpretations.

Let us therefore admit that the concept of "Universal Jurisdiction" based on the location of the Consumer of an E-Business is not a practical idea. Under this principle, no Business will ever feel confident that it is not violating the regulations of another country. It has to therefore opt for short term business policies aimed more at avoiding legal action rather than a long term brand building activity.

In order to protect Indian E-Business community therefore, it is necessary to create a "Protective Umbrella" by which application of any International Law over an Indian should be approved by a suitable authority. This principle is like what is already available in Indian law where for certain actions against the Chief Ministers, the approval of Governors is mandatory.

Obviously, this will raise a few questions on the WTO compliance and the effect of International Treaties. If the system is properly designed, it can protect all these commitments which actually fall under "Known Legal Risks" while the future manifestations of new laws that are coming up world over can be properly filtered.

CHAPTER VIII

CYBER REGULATORY STRUCTURE

Having recognized the need for regulations to promote E-Commerce, and following the guidelines of the United Nations Commission on International Trade and Law (UNCITRAL), India set about to frame regulations for Cyber Space transactions. Initially, the Ministry of Commerce, Government of India developed a draft E-Commerce Act 1998 which drew inspiration from the UNCITRAL model law for E-Commerce as well as similar legislation in Singapore. With the formation of a separate Ministry for Information Technology in December 1999, a new version of the draft E-Commerce Act was released in the form of Information Technology Bill 1999 which became the Information Technology Act 2000.

The Information Technology Act-2000, which came into effect from October 17, 2000, has envisaged the following three level hierarchies for regulation.

a) Policy Level Regulation
b) Administrative Level Regulation
c) Judicial Level Regulation

Policy Level Regulation:

The regulations concerning Cyber Space transactions in India are driven by the Ministry of Communication and Information Technology, Government of India in New Delhi. This is the common ministry which emerged after the erstwhile independent ministries namely, the Ministry of Information Technology and Ministry of Tele Communications were merged.

In due course, the Ministry of Broadcasting may also be merged with the current Ministry of Communications and Information Technology to form a common Ministry representing the convergence of technology of Information, Telecommunication and Broadcasting.

The Ministry of Law and Justice works closely with the Ministry of Communication and Information Technology in formulating the legislative policies concerning ITA-2000.

Under the circumstances, Mr Arun Shourie, the Minister in the Central Cabinet in charge of the Ministry of Communication and Information Technology heads Cyber Regulatory Structure in India at the Policy level. He is assisted by the Secretary, Ministry of Communications and Information Technology as the head of the bureaucratic structure that drives the Cyber Regulation Policies in India.

ITA-2000 has provided under section 88 of the Act, for setting up of a formal structure by which policy guidance would be available to the Ministry on a continuous basis. This committee called the Cyber Regulations Advisory Committee (CRAC) is meant to advise the Central Government either generally as regards any rules or for any other purpose connected with the Act.

According to subsection (2) to section 88 of the ITA-2000, CRAC is supposed to 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.

Accordingly, constitution of the "Cyber Regulations Advisory Committee" was notified with effect from October 17, 2000.

It consists of the following persons.

1.	Minister, Information Technology	Chairman
2.	Secretary, Legislative Department	Member
3.	Secretary, Ministry of Information Technology	Member
4.	Secretary, Department of Telecommunications	Member
5.	Finance Secretary	Member
6.	Secretary, Ministry of Defense	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	Member Secretary

In constituting this apex regulatory body, the Government of India appears to have missed an opportunity to create a body of professionals who could have provided valuable guidance to the Government on various aspects of Cyber regulations. Instead, it has opted to make it a mainly a body of the Government representatives.

The present CRAC structure has drawn resources only with a view to facilitate inter-ministerial co-ordination and inter-alia has made a cursory effort to provide a façade of non Government representation. It has failed to involve persons of eminence who could have made a real contribution to Cyber regulations at the policy level. While the interests of the industry have been represented through the industry bodies, no member of the public with necessary background and representing the interests of the Netizens has been accommodated in the committee. Even the legal fraternity is not formally represented in the committee.

The Ministry of Communication and Information technology has however initiated some steps to correct the situation by constituting adhoc working groups with a representation of Cyber Law experts in the form of members or invitees.

Hopefully, these would make up for the lack of expert representation in the CRAC.

Administrative Level:

While the CRAC forms the apex regulatory body at the Policy level, at the administrative level, the Secretary to the Ministry of Communication and Information Technology happens to be the de-facto apex official for all Cyber regulations.

Formally however, the office of the "Controller of Certifying Authorities" can be construed as the highest official acting under the ITA-2000.

According to Section 17 of the ITA-2000, the Central Government derives the power to appoint a "Controller of Certifying Authorities" (CCA) as well as "Deputy Controllers" and "Assistant Controllers" for the purposes of the Act by a suitable notification in the official Gazette.

CCA discharges the functions under the general directions of the Government and the advice of the CRAC. The deputy and assistant controllers function under the general superintendence of the Controller.

The functions of CCA as defined under Section 18 of the ITA-2000 cover the regulatory aspects concerning the operations of the Certifying Authorities and the Digital Signature regime.

Accordingly, the CCA is the licensing authority for the CAs and prescribes the necessary standards. He is the "Root Certifying Authority" for the Indian jurisdiction and issues the Digital Certificate for the CAs themselves. He also acts as a repository of digital certificates issued.

The CCA as the apex administrative authority for the CAs monitors the activities of the CAs and has the powers to revoke or suspend the licenses of the CAs if required. He has quasi judicial powers to settle disputes of CAs.

By virtue of section 69 of the ITA-2000, the CCA has the power to order interception and decryption of any information transmitted through any computer resource, if it is considered expedient in the interest of the sovereignty and integrity of India,

the security of the State, friendly relations with foreign states or public order or preventing incitement to the commission of any cognizable offence.

The CCA will have the powers to investigate contravention of the provisions of the act with powers similar to what has been granted to Income Tax authorities under the Income Tax Act-1961 including search, seizure and access to required computer data.

The Controller, the Deputy Controller and the Assistant Controller are deemed to be public servants within the meaning of the Indian Penal Code.

The first "Controller" of Certifying Authorities was appointed with effect from October 17, 2000 and this historic responsibility is being shouldered by Mr K.N. Gupta, a former director of the Department of Telecommunications.

Upon the termination of his term of three years, Mr S.Lakshminarayanan, former Additional Secretary to Ministry of Communications and Information Technology has now been given additional charge as the Controller of Certifying Authorities.

This has however created a slightly anomalous situation where an official of the Department has a quasi judicial power as Controller over NIC which is a licensed Certifying Authority.

Judicial Level

While the CRAC supervises the Policy level regulations and the CCA administers the Certifying Authorities, the "Grievance Redressal" mechanism is administered by two judicial bodies namely the "Adjudicating Officer" (AO) and the "Cyber Regulations Appellate Tribunal" (CRAT).

Adjudicating Officer:

According to Section 46 of ITA-2000, the Government has the power to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State to be an "Adjudicating Officer" for adjudging whether any person has committed a contravention of any of the provisions of the Act.

It is also prescribed that every adjudication officer shall have the powers of a Civil Court and all it's proceedings shall be deemed to be judicial proceedings within the meaning of the relevant sections of the Indian Penal Code and Code of Criminal Procedure Code.

Even though ITA-2000 became effective on October 17, 2000, it was only on March 25, 2003 that the AOs were officially appointed. In a Gazette notification dated March 25, 2003, the Secretaries in the Department of Information Technologies in each of the States and Union Territories in India have been appointed as Adjudicating Officers under Section 46 of the ITA-2000.

According to the notification, the State IT departments would provide the necessary infrastructure for the purpose and investigative support would be provided by the Local Police, the Controller and CERT-IND, the Computer Emergency Response Team sponsored by the Government of India.

The jurisdiction is based on the location of the affected Computer system within the state to which the AO belongs.

The Complaint has to be made on paper along with a fee which is 10 % of the damages claimed plus Rs 50 containing the

information such as the name, e-mail, telephone and physical address of the complainant and the respondent, the damages claimed, the time and place of contravention and particulars of fee deposited.

On receipt of the Complaint, the AO will issue necessary notice to the respondent and conduct an enquiry on an appointed date and award his decision within 6 months.

Any appeal to the order of the AO can be made to the CRAT which will be the next level for grievance redressal.

CYBER REGULATIONS APPELLATE TRIBUNAL

The "Cyber Regulations Appellate Tribunal" (CRAT) is a body set up by the Government of India under section 48 of the ITA-2000 which will hear appeals against the dispensations of the adjudicator and also the Controller of Certifying Authorities in any dispute falling under its jurisdiction.

Any appeals against the awards of the Appellate Tribunal will have to be preferred at the High Courts.

The CRAT is envisaged as a single member body with the "Presiding Officer" who has either been or is qualified to be a judge of a High Court or has been a member f the Indian Legal Service and has held a post in Grade I of that service for at least 3 years.

The presiding officer of the CRAT is appointed for a term of 5 years or until he attains the age of 65 whichever is earlier. During this tenure the salary and other benefits payable to him cannot be

varied adversely. He cannot be removed from service except by an order of the Central Government on the grounds of proved misbehaviour or incapacity after an enquiry by a Judge of the Supreme Court. Thus the office is protected from the influence of bureaucratic and political influences.

According to section 61 of the Information Technology Act 2000, Civil courts will not have jurisdiction to entertain any suit or proceedings in respect of any matter which an adjudicating officer or the Appellate tribunal constituted under the act is empowered to determine and no injunction can be granted by any court or other authority in this respect.

The offices of the Adjudicating Officer and the CRAT are aimed at providing a speedy disbursal of Cyber Justice from a set of officials who are trained IT specialists. They have also been provided the freedom to determine their own procedures for the conduct of their operations.

It is therefore expected that the ITA-2000 will now be seen in operation at the ground level and the public would be able to appreciate the Cyber regulatory regime. Hopefully this should provide the necessary confidence to the E-Business community so that they can expand their business both within India and elsewhere.

CHAPTER IX

CYBER CRIMES

Internet was born free and for the purpose of communication against all odds. In the initial days, it grew in popularity amongst knowledge seekers and established itself as the Information Super highway. However, as mankind started understanding the enormous strengths of a global system of instant electronic communication, Internet came to be used more and more for commercial applications.

The commercialization of Internet was beneficial to the society in one sense since Internet could be used for efficient delivery of many services including Banking, Selling of Electronic Products etc. With the growth of such E-Commerce, also grew the activities of anti society elements who tried to exploit the Internet infrastructure for indulging in Crimes of various types.

It is the growth of Commercial interests and the threat posed by criminal elements that forced the development of regulatory mechanisms.

Cyber Crimes therefore became the focus of Cyber Laws and addressing such concerns was one of the main objectives of ITA-2000.

Before we try to understand how Indian Cyber regulatory system has tried to address the same, it would be useful to classify various actions of Netizens which are commonly understood as Cyber Crimes.

The classification itself can be done with different perspectives. If we keep a broad perspective, we can define "Crimes" as "Deviant

Behaviour from the norms of a society" and in this context, any action that is deviant of the accepted behavioural norm of a "Cyber Society" can be called a Cyber Crime.

In the narrower perspective, we can define "Crimes" as "Acts of omission and Commission defined by the laws of a jurisdictional force as punishable acts".

In this context, the definition of Cyber Crimes in India has to be restricted to what have been identified by ITA-2000 as acts deserving punishments or penalties of some kind. These are Cyber Crimes of the first order.

Out of the deviant actions not identified by ITA-2000 as offences, are some which are already defined by the Meta Society as "Crimes" under other legal provisions such as the Indian Penal Code. If such crimes are committed using "Cyber Tools", they can also be classified as "Cyber Crimes" but can be referred to as "Cyber Crimes" of the second order.

Another set of actions that can be called Cyber Crimes of the third order are those which have been specifically declared as punishable offences in the statutes of some of the other civilized countries though not so classified in India.

The First Order Cyber Crimes (FOCC) will be punishable under the provisions of ITA-2000 while the Second Order Cyber Crimes (SOCC) will be punishable under IPC or other appropriate statutes using Cyber documents as evidence.

The Third Order Cyber Crimes (TOCC) will only be punishable if the Country in which the subject action is a declared offence is able to lay its hand on the person or property of the offender.

International Cyber Crime treaties will be relevant in such a context.

In a different perspective, we can also classify Cyber Crimes from the angle of the effect of the offence on an individual or property. Accordingly, there could be Crimes against "Property" and Crimes against "Persons" and the "Property" or "Person" could be belonging either to the Meta Society or to the Cyber Society.

It is also essential to remember that when we talk of Cyber Crimes we not only deal with crimes committed over Internet but also crimes committed using any "Electronic Document" or a "Computer".

We shall discuss all these different categories of Cyber Crimes in different chapters of this book. While this chapter will mainly discuss Cyber Crimes under ITA-2000 and to some extent under IPC, which are the Cyber Crimes of the first and second order described above, the chapter on Intellectual Property Issues as well as on Privacy and Freedom of Speech Issues cover the Crimes against Virtual Property and rights of personal rights which are outside the domain of ITA-2000 but fall under the category of Cyber Crimes of the third order.

CYBER CRIMES UNDER ITA-2000

The declared objective of ITA-2000 was to facilitate E-Commerce. In view of this, the Act seems to focus more on offences that directly affect E-Commerce. In the bargain, it may appear that ITA-2000 is lenient on other crimes of graver nature.

However, if one remembers that Section 4 of ITA-2000 extends the applicability of any other law applicable to written documents to Electronic documents, it is clear that any crime other than

those described in ITA-2000 would be equally enforceable even when it has a shade of Cyber Crime involved in it. The amendments made to IPC and the Indian Evidence Act consequential to the passage of ITA-2000 ensures that such crimes do not go unpunished.

It is therefore considered acceptable that ITA-2000 restricts itself to one set of Crimes only which we have described as First Order Cyber Crimes.

PENALTIES AND OFFENCES UNDER ITA-2000

ITA-2000 discusses consequences of deviant behaviour of a member of a society under two distinct chapters.

Chapter IX of the Act covers actions that create liabilities for imposing "Penalties" on the offender by way of compensation payable to the victim.

Chapter XI discusses actions that can be classified as "Offences" where there could be imprisonment and fine payable to the Government.

Chapter IX offences can be adjudicated by an Adjudication Officer appointed by the Government.

Chapter XI crimes can be prosecuted by the law enforcement officers as prescribed by the Act and in the Criminal Procedure Code.

In ITA-2000, Section 43 is a very significant section which covers a broad section of typical Cyber Crimes. This section provides a financial remedy to a victim to the extent of R 1 crore as compensation for damages suffered.

It is imperative however that the damage claimed may have to be proved to the satisfaction of the relevant judicial authority and cannot be arbitrary.

Section 43 states thus:

> If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
>
> (a) accesses or secures access to such computer, computer system or computer network;
>
> (b) downloads, copies or extracts any data, computer 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 contaminant or computer virus into any computer, computer system or computer network;
>
> (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
>
> (e) disrupts or causes disruption of any computer, computer system or computer network;
>
> (f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
>
> (g) provides any assistance to any person to facilitate access to a computer,

computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(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 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 formalized 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 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 section will become operative only in the event of the offensive act being committed "without the permission of the owner or the person in charge of a computer System".

It is therefore important for the person claiming the damage to disprove and the person defending the charge to prove the existence of any "Permission".

"Permission" in such context can be expressed or implied and is influenced by the normal practices adopted by persons in similar circumstances.

The actions covered by the section are

a) **Securing access to the System**

For invoking this section, it is sufficient if the offender "Secures Access" "Without Permission" and creates a "Damage". There is no need to prove existence of "Intention to cause damage".

It is interesting to note that under Section 66 of the Act, the offence of "Hacking" has been defined which has some similarities to this section, since "Hacking" also may include "Unauthorized Access". However, for "Hacking" to be invoked, existence of Mens Rea or "State of mind indicating culpability" is essential and may cover loss of information assets without "Securing Access", if such cases can be conceived.

b) **Downloading, Copying or extracting any data**

This is a fairly wide provision that can be applied to any situation where data has been extracted "Without Permission".

It is interesting to note that the section even covers data stored in any removable storage medium. It may however

be necessary to consider this provision applicable only when such a "Removable Storage Media" is part of the Computer or Computer System or Computer Network and not otherwise.

The use of the word "Copy" in this section has often led to the interpretation that this section can be applied to "Copyright Violations".

This view however seems to be an optimistic extension of the intended meaning of the section. It must be considered in the context of the section that the violation refers only to the case where copying of data occurs without the permission of the "owner of the Computer" and not of the "Owner of the Copyright of the Data".

c) **Introducing a computer Contaminant or Virus**

Considering the importance of Virus in the context of Computer Crimes, it appears that this provision hidden in the sub clause of the section 43 is of great consequence to the observers of Cyber Crimes.

It is necessary to observe the explanatory note to the section which defines the "Computer Contaminant" and "Virus".

While a "Computer Contaminant" includes any set of instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, a "Computer Virus" includes any computer instruction, information, data or programme that adversely affects the performance of a computer resource.

d) Damaging data or the System

It is essential to reiterate that even an "Unintentional" or "Accidental Damage" to either the hardware or a software can be covered within the meaning of this subsection.

e) Disrupting or Causing Disruption to the System

While this sub-section may perhaps cover a person committing a "Denial of Service" attack on a network, it is hard to exclude the innocent owner of a "Zombie" computer involved in a "Denial of Service Attack".

f) Blocking access to another authorized user

This provision could cover various provisions including a case where the password to an e-mail account of a subject victim is altered by a culprit.

g) Assisting another person in contravening provisions of the law

This is an interesting provision that could even be extended to any person who negligently handles his password or a system security feature to commit a contravention.

h) Charging service availed by him to another person by tampering with or manipulating the System

This provision is intended to cover Credit Card related frauds or Internet Access right thefts. However, if it involves "Tampering or Manipulating" the system then such offences may also qualify as "Hacking" under Section 66 of the Act.

As one can observe, Section 43 of the ITA-2000 is as good as a whole chapter on Cyber Crimes and in the days to come would be one of the most hotly debated sections across the table of an Adjudicator.

Within Chapter IX, section 44 addresses another type of offence which covers "Failure to furnish returns..etc". This is basically aimed at Certifying Authorities furnishing returns to the Controller of Certifying Authorities.

It must be noted however that the section can be used by the Controller against any other authority whom he has directed to produce any document and by a logical extension can be invoked by a Certifying Authority against a subscriber to Digital Certificate. Penalty under this section can be up to RS 5000 for every day of default subject to a maximum of Rs 1.50 lakhs.

OFFENCES UNDER CHAPTER XI OF ITA-2000

Chapter XI of the ITA-2000 lists a few offences which could result in imprisonment and fine for the offender.

Amongst the principle sections of the chapter are Section 66 which covers "Hacking", Section 67, which covers "Obscenity".

Section 65 covers "Tampering With Source Codes" which is an offence covering "Tampering of Evidence".

Section 70 covers special provisions regarding an attempted intrusion of a system declared as "Protected System".

Sections 71, 73 and & 74 cover different aspects covering a Digital Certificate user and his responsibilities.

Sections 68 and 69 indicate certain powers given to the Controller to issue directions and the consequences of their violation.

Section 72 covers the responsibilities of authorities such as the Certifying Authority in respect of information of the public which comes into their hands and the consequences of the breach of privacy and confidentiality.

Each of these offences are discussed in greater detail below.

Tampering of Computer Source Documents:
Section 65 of the ITA-2000 states,

> "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."

The use of Computer source documents in this section appears to relate to records such as "Access Log" maintained by ISPs, "Mail box usage" information, "History of Web sites visited" by a user in a Corporate or Cyber Cafe network, etc. and not to the software source code as we normally understand.

The section also says that the offence is recognized only "When a Computer Source Code is required to be maintained by law".

This section is essentially to assist the law enforcement authorities to ensure that critical evidence of a crime is preserved.

However, neither the Controller nor the Government has yet notified the "period" up to which different types of records are to be maintained. Hence normal prudence has to be followed to determine the reasonable period up to which evidence sensitive computer records should be maintained by a system administrator.

In Europe, there is a demand that the information has to be preserved up to 7 years. This gives an idea of what the law enforcement authorities think elsewhere. In respect of financial disputes, the limitation period accepted in Indian law is 3 years. If we add the normal judicial delays, one can say that a period of 7 years is a good time up to which the information may have to be preserved.

Hacking with a Computer System (Section 66)

Hacking is one of the most commonly referred to term when we discuss Cyber Crimes. ITA-2000 has introduced a "Definition" for the term hacking, under section 66. It states,

> (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.

It is interesting to note that prior to this legal definition of'Hacking", the Cyber society had its own understanding of the term. The term was often used to mean "Unauthorized Access to a Computer System", but there was always a distinction between the terms "Hacking" and "Cracking".

The group of technology specialists who indulge in "Unauthorized Access" for the purpose of exploring security loopholes in systems and software and do not have any intention of damaging the data or otherwise use the access for illegal gratification called themselves as "Ethical Hackers". Those who indulge in "Unauthorized Hacking" for criminal purposes or for damaging the data in a Computer system were called "Crackers".

Relatively speaking, Hackers were a respected community of security specialists while Crackers were outlaws.

The dividing line between hackers and crackers have always been thin and often people on the Hacker side transgressed the yellow line. However the concept of a Cracker being evil and a Hacker being a friend of the society was useful to channelise the resources of Computer specialists to the betterment of the society and reform many who start as crackers at a young impressionable age and later become hackers of repute.

Sec 66 of the ITA-2000 has however redefined the universal understanding of the term and in the context of our discussions of Cyber Crimes in India, we shall therefore use the term "Hacking" as a Crime as defined. This would go along with the society's understanding of Cracking. Where necessary, we shall

use the term "Ethical Hacking" to distinguish between the erstwhile hacking and Cracking.

The essential requisites for an act to be defined as "Hacking" in India are as follows.

- There should be an intention to cause a wrongful loss or damage to the public or any person or
- .There should be knowledge that the act is likely to cause a wrongful loss or damage to the public or any person And
- There should be destruction of or deletion of or alteration of or diminution in the value of or diminishing in the utility of any information residing in a Computer source.

The section uses the words “By Any Means”. This is amenable to be interpreted as suggesting that the actual means through which the loss to the information asset was caused is immaterial.

Thus "Hacking" can be invoked even where it is done by a person who is otherwise authorized to access the Computer information. It can be extended to acts which involve non Cyber crimes such as physical destruction of the Computer Network resulting in damage to the Information or conspiracy and fraudulent acts inducing another person to destroy the information without his knowledge.

"Ethical Hacking" (Access without intention to cause loss and without the knowledge that loss would be caused) falls under Sec 43 and if such act does not cause any loss to any person, it would not result in payment of any damages. It is however debatable if in case of any “Ethical Hacking” the defence of “No Knowledge” is acceptable.

"Cracking" or "Hacking" as per ITA-2000 could result in invoking of both Sec 66 and Sec 43. Since Sec 66 is a prosecution case and Section 43 is a case by the victim, they may be concurrently applied without inviting the principle of Double Jeopardy.

The definition of "Hacking" as used in the Act is very broad and can be used for most of the Cyber Crimes including Virus introduction, Denial of Service etc which are also covered under Sec 43 of the Act.

Publishing of Information which is Obscene

Section 67 of the ITA-2000 prescribes that

> whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to prurient interest, or if its effect is such as 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 punishable with imprisonment in the first instance up to 5 years and fine up to Rs 1 lakh. In subsequent convictions, the term of imprisonment can extend to 10 years and fine may extend to Rs 2 lakhs.

It may be observed that what is an offence is "Publishing" or "Transmission". Viewing of an Obscene content by itself is not an offence. "Causes to be published" means that the liability is that of the Owner of the Content or the facility and not that of the agent or employee who may be involved as an intermediary.

Further the offence would materialize only if the content is likely to "deprave or corrupt" persons to whom the content is likely to be exposed in the normal course. In effect, what may be an offence if the site is meant for Children's view may not be so if it is meant for adult view.

This section is one of the most controversial parts of the Act since the definition of the terms "lascivious" or "Prurient Interest" etc are vague and are capable of being interpreted in different ways in different societies. Since the Act is applicable not only in India for contravention committed outside India (Sec 75) also, this section is likely to be a bone of contention if the Act is tried to be applied to people outside India.

Already several cases have been registered by the Police in India on many Cyber Café owners for allowing viewing of Obscene web content. A PIL Case was also filed in Pune by a lawyer on Rediff.com alleging that the search engine service provided by the portal gave links to pornographic sites. Another case was filed by the Delhi Police on Times of India for obscene web content having been hosted by one of their members to the "Free Web Page Service".

The role of intermediaries such as the Cyber Café or the Internet Service Provider as to the content passing through them is discussed in greater detail in a subsequent chapter.

In most of the cases that have been launched under what is generally described as "Cyber Pornography", Cyber Café owners have been charged of facilitating viewing of pornographic web sites. The charges have been mainly framed under section 292 of the Indian Penal Code applicable mainly for obscene material in print form. Since "Viewing" of an obscene web site cannot be held as an offence, and the Cyber café owner is neither the

publisher nor the distributor of the offending web content it is doubtful if the cases against the Cyber café owners are maintainable.

OFFICIALS/PARTNERS TO BE RESPONSIBLE

Businessmen and Professionals such as Partners, Directors, Managers and Company Secretaries should beware that if any offence is committed by their Company or Firm, any person who was in charge at the time the offence was committed, and was responsible to the company for the conduct of the business, may also be held liable. (Section 85)

The Case of Dr L Prakash of Chennai

The case of Dr L Prakash of Chennai who has been accused of facilitating pornographic web publication has been one of the most publicized cases in India in recent days under the Cyber Crime category.

In this case, Dr L Prakash, a noted orthopedic surgeon in Chennai was accused of having procured obscene pictures by coercion as well as other illegal means and causing it to be published through web sites owned amongst others by his brother in USA.

The case has highlighted how complicated is the investigation and prosecution of an alleged offence which has both Cyber and non Cyber elements.

Can an Indian Maintain a Porno Site?

The passage of the ITA-2000, has opened a question mark on whether Indians elsewhere in the world can be punished for offenses under Sec 67 of the ITA-2000 even though such an activity may not be a crime in the country in which they are living.

According to Sec 67 of the ITA Act "Publishing", "Transmitting" or "Causing to publish" in electronic form any obscene material is a punishable offense. The penalty is stiff with a possibility of imprisonment up to 5 years even for the first offense.

According to Sec 1(2), of the Act

The provisions of ITA-2000 extends to

> "the whole of India and, save as otherwise provided in this Act, it applies also to any offense or contravention there under committed outside India by any person"

Further expanding on the applicability of the Act, Sec 75 states as follows:

> (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offense or contravention committed outside India by any person irrespective of his nationality. .
>
> For the purposes of sub-section (1), this Act shall apply to an offense or contravention committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India

In view of Sec 81 which states

"The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force",

the provisions of the ITA-2000 becomes applicable to both Citizens of India and others whether they are living in India or not.

If therefore an offense is committed under the Act and the person is under some control of the Indian Government, such as having a passport issued in India, it is likely that the person may be brought to book even though the "Offense" committed may not be an "Offense" under the law of a foreign country where the Indian citizen may be residing.

Under section 75, the applicability is conditional to " the act or conduct constituting the offense or contravention involving a computer, computer system or computer network located in India". This provision is more appropriate to describe a "Hacking" offense. However, in the context of "Causing transmission" of an obscene material, any act including "Providing access to the Internet" may be construed as "Using a computer network in India".

It can therefore be surmised that "No Indian Passport holder should dare to contravene the ITA-2000" since he runs the risk of being extradited and imprisoned.

Does this restrict an Indian from maintaining a pornographic site outside India?.. Practically Yes, unless the site owner has taken reasonable steps to block Indian visitors from visiting the site.

If so, what would be a reasonable step?

Blocking the IP addresses of Indian ISPs? Or
A request to the Indian Government to block access to the site from Indian ISP s?
Will a notice "This site is not meant to be viewed by

Indians. The management of the site is not responsible for any Indian viewing the site..etc be sufficient?.. are some of the issues that arise.

The situation here is similar to the French Government's case against Yahoo- Nazi Memorabilia site.

The larger issue is "Whether the Indian National Government can impose itself on the Cyber activities of a person (Indian or Non Indian)" outside the geographical jurisdiction of India? And Is it practical to extend the jurisdiction of the Non Cyber Society to the Cyber Society across borders?

..For the time being, there may not be final answers to these questions. There can be only opinions.

Blocking of Pornographic Sites

Quite often the regulators in India have come across requests to block websites which violate the local law. Some of them are terrorist supported sites that cause a threat to the integrity of the nation. Other than these, there is also a constant demand from a section of the community that websites which have pornographic content should be blocked at the ISP level.

In a public interest litigation concerning the "Protection of Children from Pornographic Content" which the Mumbai high court had an opportunity to consider, the Mumbai Police held out that it is technically not possible to block pornographic sites at the ISP level and instead there should be a stricter monitoring of Cyber Cafes who allow children to access Pornographic websites.

The recent developments in China and Pakistan however indicate that certain measures however imperfect they can be, are effective

at ISP level to block pornographic websites. They would work like most of the Spam filters, filtering most of the known pornographic content and substantially reduce the incidence of Pornographic content distribution in India.

In order to introduce a formal system by which the Government can consider requests for blocking of specific websites (easily applied to terrorist sites but can also be applied in principle to Pornographic sites) the Ministry of Information Technology has notified on 27th February, 2003 that CERT-IND (Computer Emergency Response Team) will be the nodal agency to decide on the modalities of blocking any website and they can be approached through the Controller or other designated officials such as the IT Secretaries in States or the CBI (Central Bureau of Investigation) etc.

Failure to Comply with Controller's order

Under Section 68 of the Act, the Controller is empowered to direct a CA or any employee of such authority to take such measures or cease carrying on such activities as specified in the order. Failure to comply with such order may result in imprisonment up to three years or to a fine not exceeding two lakh rupees or to both.

Interception and Decryption of Messages.

Under Section 69, the Controller has the powers to order interception of any communication, or decryption of any encrypted electronic document, hand over of encryption/decryption keys etc..

...if it is considered expedient to do so 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.

If any person who is in charge of a Computer system fails to assist any Government agency in decryption of any message, he may be liable for imprisonment up to 7 years.

There is however a guideline issued by the Department of telecommunications to the Internet Service Providers where the telecom authority has retained rights for ordering interception and blocking of web sites. Even though the Telecom Ministry has now merged with the IT ministry and convergence laws are in the offing, the exact procedure for ordering interception of communication and its monitoring is still not clearly defined.

Interception of Communication under ITA-2000, CCB-2002 (Proposed) and POTA-2002

(Ed: CCB 2002 has been shelved for the time being though it maybe taken up again)

According to ITA-2000, the "Controller of Certifying Authorities" has been given a power to direct interception of any electronic communication under certain conditions.

Section 69 of ITA-2000 states ::

> **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 in charge 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.

This section stipulates the conditions under which the power of interception can be exercised and mandates that the Controller has to record the reasons and give a written order to an agency ..such as the Police to intercept any information transmitted through a Computer resource.

This section does not provide any special powers to the Police but only stipulates that they need the written order of the Controller before any interception can be made. Since interception of electronic communication is to be done at the ISP level and using "Decryption" of messages in some cases which may need the support of the Certifying Authorities (CA), this provision is meant to protect the ISP s and CA s from direct interference by the Police.

From the point of view of the Police this section actually restricts their powers by making it subordinate to the wishes of the Controller.

The Ministry of telecommunications before it merged with the IT Ministry had also prescribed outside the statute, a power for "Interception" through the Telecom guidelines for setting up of submarine landing stations

This guideline stipulates that the "Licensee" (i.e. the ISP) will have to make all technical provisions to enable interception and filtering of internet data passing through the ISP at his cost and

also provide physical space for the monitoring authority within the ISP premises to carry on its work of interception and filtering. It also mandated that the ISP will not allow bulk encryption by ISP s and others would be restricted to encryptions of 40 bit key length in RSA algorithms.

This provision again does not provide any special power to the police but only empowers the administrative machinery in the Government to order interception through the Police if need be.

In the proposed Communication Convergence Bill (CCB) which is pending in the parliament for being passed into a law, the relevant provisions on interception state as follows.

Section 66. of Communication Convergence Bill::

Interception of communication and safeguards.

(1)Subject to the prescribed safeguard, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government, on the occurrence of any public emergency or in the interests of the security, sovereignty and integrity of India, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, may direct:
(i) any agency of that Government to intercept any communication on any network facilities or services;

(ii) any service provider that any content brought for communication by or communicated or received by, him shall not be communicated or shall be intercepted or detained or shall be disclosed to that Government or its agency authorized in this behalf:

(2) The service provider shall, when called upon by any agency, which has been directed to carry out interception under sub-section (1), extend all facilities and technical assistance for interception of the content of communication.
(3) Any service provider who fails to assist the agency referred to in sub-section (2) shall be punished with imprisonment for a term, which may

extend to seven years.
(4) Save as otherwise provided under this section, any person, who intercepts any communication or causes any communication to be intercepted or discloses to any person, any content shall be punishable with imprisonment which may extend to five years or with fine which may extend up to ten lakh rupees, and, for a second and subsequent offence, with imprisonment which may extend to five years and with fine which may extend up to fifty lakh rupees .

Explanation: For the purposes of this section, "interception" means the aural or other acquisition of the content through the use of such devices or means as may be necessary for such acquisition.

Section 67 of Communication Convergence Bill:

Nothing in this Chapter shall affect the provision of section 69 of the Information Technology Act,2000.

This section again provides the enabling power for the Central or State Government to order interception in emergent situations and applies to communication other than what is covered under Section 69 of the ITA-2000.

What is to be noted is that sub section 66 (4) of CCB prescribes a punishment for any interception other than what is authorized as per the section. This can perhaps be used against a Police officer also in case he intercepts a communication without the order of the appropriate official as envisaged by this act. In fact ITA-2000 provision appears incomplete compared to the provisions of the Communication Convergence Bill.

Having seen that neither the ITA-2000 nor the Communication Convergence Bill provides any power to the Police to "Intercept" communication, let us now see what the POTA (Prevention of Terrorism Act) has stated in this regard.

Chapter V of the POTA has been dedicated to the powers of interception.

POTA has approached the issue of interception in a detailed manner unlike in the earlier cases. The act defines "Electronic Communication" and "Interception".

According to Section 36 (b) "Intercept" means the aural or other acquisition of the contents by wire, electronic or oral communication through the use of any electronic, mechanical or other device.

Under Section 37, a "Competent Authority" is defined to exercise the powers of interception, who would be an officer not below the rank of Secretary to the Government in the case of State Government and not below the rank of Joint Secretary to the Government in the case of Central Government.

Section 38 stipulates that a police officer not below the rank of Superintendent of Police supervising the investigation of any terrorist act under this Act may submit an application in writing to the Competent Authority for an order authorizing or approving the interception of wire, electronic or oral communication by the investigating officer when he believes that such interception may provide, or has provided evidence of any offence involving a terrorist act.

The particulars required to be submitted for making such a request has also been stipulated elaborately under Section 38 (2) of the Act. The request has to be substantiated with additional information which the competent authority may call for. The permission when granted will also be for a limited time period not exceeding 60 days at a time.
It must be noted that the Competent authority may reject the application of the Police officer,. Further, the competent authority

himself has to submit a copy of the order to a review committee within 7 days for approval.

The act also stipulates that "An interception may be conducted in whole or in part by a public servant, acting under the supervision of the investigating officer authorized to conduct the interception".

Thus, the powers of interception envisaged by POTA is well regulated both at the time of interception and its monitoring.

Emergency powers of interception are however granted under Section 43 of the Act to an Additional Director General of Police or a police officer of equivalent rank. Such powers are to be exercised in designated emergent situations such as defined in the section and to be recorded in writing.

The emergent situations refer to situations such as

(i) immediate danger of death or serious physical injury to any person; or
(ii) conspiratorial activities threatening the security or interest of the State; or
(iii) conspiratorial activities, characteristic of a terrorist act, that requires a wire, electronic or oral communication to be intercepted before an order from the Competent Authority authorizing such interception can, with due diligence; be obtained, and there are grounds on which an order should be issued under this section to authorize such interception,

Such orders should be referred to the Competent authority within 48 hours and in case of rejection will cease to be effective and the officer may have to face the consequences of violating the provisions of the Act which may result in imprisonment of the

Police officer for a period of up to one year and fine of up to Rs 50,000.

The Act also provides for protection of the information collected and for their admissibility as evidence .

POTA therefore provides a well thought out procedure for interception and management of information collected through such interception. It is not correct to say that it gives draconian powers to the Police since the checks and balances are present in the act itself.

What is to be remembered is that the provisions of POTA will override the provisions of ITA-2000 whenever it is invoked and therefore the procedures mentioned herein become relevant even for interception of Internet data.

Protected System:

Under Section 70, the Government can also declare by a notification, any Computer as a "Protected System" and specify the authority to access such systems through an order in writing. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section is punishable with imprisonment for a term which may extend to ten years and shall also be liable for fine.

The Government is however yet to notify any system under this section as "Protected System". It is expected that the systems of the defense establishments or atomic energy commission etc may be declared as "Protected Systems" under this section.

Misrepresentation for Getting Digital Certificate

Under Section 71, any person who makes a misrepresentation to or suppresses any material fact from the Controller or the CA for obtaining any license or Digital Certificate shall be punishable with imprisonment that may extend to two years and/or with a fine that may extend to Rs 1 lakh.

Penalty for Breach of Confidentiality and Privacy:

Sec 72 is another section where the inappropriate heading has caused some confusion even amongst many experts in Cyber Law field. This section talks of "Breach of Confidentiality and Privacy" which are "Human Right Concerns" the world over. Some have interpreted this section as trying to preserve such Privacy rights of individuals.

However, this section is limited to imposing a statutory

responsibility on Certifying Authorities and the Controller who are likely to come cross sensitive personal information of individuals during the course of their functioning. Accordingly, if any person who in pursuance of any of the powers conferred under this Act, has secured access to any information, discloses such information without the consent of such person, he shall be liable for imprisonment up to 2 years and or fine up to Rs 1 lakh.

False Digital Certificate

Under Section 73, if any person publishes a Digital Certificate which is false, already revoked or suspended, (unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation) can be punished with imprisonment that may extend to two years or with fine which may extend to one lakh rupees or whit both.

Publication of Digital Certificate for Fraudulent Purpose:

Under Section 74, if any person knowingly creates or publishes or otherwise makes available a Digital Certificate for any fraudulent or unlawful purpose, he may be punished with imprisonment up to two years and/or with fine up to Rs 1 lakh.

DETERMINATION OF THE PENALTY

In determining the penalty or punishment under the Act, the fact whether the offence was the first or a repeat offence, the extent of benefit gained by the guilty and the loss caused to the affected persons would be given due consideration.

According to Section 45 of the Act, where no penalty has been mentioned in the Act for any contravention, a penalty not

exceeding Rs 25000 would be applicable.

In addition to the above penalties, any computer or an accessory used in the contravention of law is liable for confiscation. Also, not withstanding the punishment or penalty imposed by the act, the offender may also be liable under any other provisions of law.

According to Section 77 no penalty 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.

While this suggests that a person can be tried for the same offence both under ITA-2000 and another Act,

According to Section 81 of the Act the provisions of this Act will have effect not withstanding anything inconsistent therewith contained in any other law for the time being in force.

JURISDICTION

We have discussed some aspects of Jurisdiction in the earlier chapter on Digital Contracts. The discussion is extended here into a few other areas of relevance both with reference to the ITA-2000 as well as two important case laws that have arisen in the International market.

Being a law formed under the UN guidelines, ITA-2000 has been made applicable to the whole of India including Jammu and Kashmir.

Further, as per the provisions of Section 75, the act will also apply to any contravention and offence committed outside India

by any person irrespective of his nationality, if the act constituting the offence involves a computer, computer system or computer network located in India.

As per section 61 of the ITA-2000, 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

The offences coming under Chapter XI of the Act are directly coming under the jurisdiction of a criminal court and not under the adjudicator and the Cyber regulations Appellate Tribunal.

Two landmark Judgments on Jurisdiction

Discussion on Jurisdiction in Internet Space would be incomplete without reference to two important judgments one in California and the other in Australia.

In the Metro-Goldwyn-Mayer Studios, et al. v. Grokster, Ltd., et al case heard at United States District Court For the Central District of California Western Division, the Court considered a Copyright infringement lawsuit arising out of Sharman's distribution of its file sharing software to California residents, and their subsequent use of such software.

In this case, the Court held in its decision published in January 2003 that that Sharman Network Ltd. ("Sharman") a company based in Australia which distributes software that enables individuals to utilize the Kazaa peer-to-peer file sharing network,

and LEF Interactive PTY Ltd. ("LEF"), which manages Sharman's operations, **are subject to personal jurisdiction in the California federal courts.**

The court reached this conclusion notwithstanding the fact that Sharman's activities all occur outside California, where it operates a web site from which California residents download the Kazaa software. The Court found that Sharman had purposely availed itself of the privilege of doing business in California by permitting its software to be downloaded by a significant number of California residents for Sharman's financial benefit.

The High Court of Victoria heard a defamation suit filed by a businessman Mr Joseph Gutnick Vs Dow Jones & Co Inc of USA. The allegation was that Dow Jones operates a subscription news site http://www.wsj.com which carried an article entitled "Unholy Gains" containing defamatory references to Joseph Gutnick.

The Court in its judgment delivered in December 2002, held that because the alleged damage to Mr. Gutnick's reputation occurred in the Australian state of Victoria, where he lives, it is appropriate that it has jurisdiction, even though the article had been distributed from servers in New Jersey.

These two cases clearly establish the current judicial thinking that Internet jurisdiction can extend based on the residence of the victim. This principle is also enshrined in the ITA-2000 under Section 75 as well as the laws of many other countries.

Conviction Across Borders

In pursuing conviction of any accused, if the person is outside India, there is a need to invoke International Treaties with

appropriate procedural compliance. Normally such treaties provide for extradition if the offence is also an offence in the other country and a Court in India has already found the accused prima-facie guilty of the crime. Different countries in Europe and the American continent are forging Cyber Crime Treaties to ensure mutual cooperation in investigation of Cyber crimes and prosecution of criminals. There is also an attempt through the "Hague convention" to remove the clause of "Duality of Offence" and accept the verdict of a Court in one of the member countries as sufficient cause for seeking extradition.

India is presently not a member of any of the Cyber Crime Treaties including the Hague Convention.

However, India has mutual extradition treaties with many countries and is also a member of TRIPS (Trade Related Aspects of Intellectual Property Rights) Agreement under the WTO (World Trade Organization initiatives. In view of TRIPS, India is a party to the global efforts at harmonization of laws regarding Copyright, Trade Marks, Patents etc.

CHAPTER X

INTELLECTUAL PROPERTY ISSUES

Information Technology Act-2000 (ITA-2000) was introduced with the three pronged objective of

Promoting E-Commerce
Protecting Netizens
Punishing Cyber Criminals

The Act however did not cover Intellectual Property Issues in Cyber Space such as Domain Name Disputes arising out of Trade Mark Rights or otherwise, Copyright Issues and Patent Issues that affect Virtual Properties .

Similarly the Act did not address the issues of "Rights of a Netizen" such as Cyber Stalking, Spam, Freedom of Net Speech etc.

All offences concerning these rights as well as "Harassment", "Threat", "Intimidation" etc through e-mails or web sites should therefore be covered as offences under the Indian Penal Code supported by Electronic Documents as evidence as provided by the amended Indian Evidence Act or any other relevant legislation.

Since some of these issues are important for all Netizens, a brief coverage of some of the IPR related issues relevant to the Cyber Laws of India are discussed here.

It must also be remembered that just as Section 75 of the ITA-2000 makes any person outside India also liable for punishment under the Act, many other countries have passed laws stating that their laws are applicable to persons outside their country. Hence some of these legal issues become relevant for our study even though they are beyond the scope of ITA-2000.

DOMAIN NAME DISPUTES

Domain Names are the descriptive names of web sites that a Netizen enters in the Browser window to reach the web site. Examples of the names are www.naavi.org or www.ceac4india.com Even though all Computers connected to the Internet are technically identified by the IP address which is a four quartet number, the domain name itself is more user friendly.

Hence, the Internet works on a system of Domain Name Management where each of the Website hosting computers which are accessed by public are also registered with a more easy to remember name. The link between the name and the IP address is maintained by the Domain Name Service providers through a Domain Name registration mechanism.

The apex name and number managing authority called ICANN (Internet Corporation for Assigned Names and Numbers) allocates the IP addresses to designated service providers and appoints "Domain Name Registrars" who allocate the available IP address to the public against a required name.

Top Level Domain (TLD)

These domain names have an extension such as .com, .org or .net which are called "Top Level Domains".(TLD) The actual domain name of a web site is a combination of the directory www, the distinguishing name such as Naavi and the top level name extension.

In order to provide several options of names, ICANN has introduced several generic TLD s such as .com, .net,.org,.info, .biz, .name etc. Additionally extensions such as .co.in or .co.uk, .com.sg etc are made available through country wide registrars as "Country Code TLDs" (ccTLDs). In India, NCST (National Center for Software Technology) manages the allocation of the ccTLDs for India that ends with .in.

Domain Name Registration

Technically speaking, available domain names subject to some technical limitations (such as maximum number should not exceed 67 letters, not to contain space etc) are issued on a first cum first served basis by a registrar upon payment of a contract fee for a period of one year to 10 years.

The owner of the domain name is called the "Registrant" The registrant also designates three types of persons to interact with the registrar on behalf of the registrant. They are the "Administrative Contact", "Technical Contact" and the "Billing Contact" for each of the purposes that the name indicates.

During this time of registration, the given name is linked to a specific IP address in the network of Domain Name Servers across the globe that serve the Netizens.

In case the owner of the domain name i.e. the "Registrant" wants the IP address linked to the name be changed, it is effected by the registrars.

In case the name is not renewed after the expiry of the contract period, the name is often allotted to any other person who may apply subsequently.

Alternate Domain Name Management Authorities

Outside the ICANN network, a few enterprising organizations have evolved to provide domain names beyond the authority of the ICANN. New.net is one of the private operators who enables several TLD extensions of their own such as .shop, .mp3, .law etc through a software plug-in for the browser that can be down loaded from the Internet. They are said to have created over 144 million Netizens who can resolve the domain names provided by New.net.

Recently one more such operator viz., dotworlds.net has started registering domain names with extensions such as .usa, .texas etc accessible using its own downloadable browser plug in.

Similarly OpenNIC, AlterNIC, ADNS.net are other agencies which offer their own TLDs. They maintain a separate DNS server system which is capable of resolving these names. The browser will have to refer to these Domain Name Servers when the domain name entered in the address bar finds no match at the ICANN maintained domain name server.

Obviously, if any of these Alternate Domain Name Authorities start issuing TLD s similar to what ICANN is issuing, there will be a collision of domain names. Recently such clash was observed when ICANN chose to accredit usage of the TLD .biz which was

already in use by some of the other operators. Not able to counter the power of ICANN, the other operator has now taken steps to change the registrations made earlier with the .biz extension.

More such conflicts between different Domain Name Authorities cannot be ruled out in future unless a proper mechanism is evolved to bring all the Domain Name Authorities under some form of common regulation.

Domain Name as a Virtual Property

Even though the technical nature of a domain name is nothing but a registration link, in view of the importance of the domain name in identifying a website, it has today come to be recognized as a "Virtual Property" much like a brand name.

Domain Name Disputes

As a result, whenever two domain names appear similar, the more popular domain name owner feels that there is an attempt by the other to unfairly benefit by his brand name and also that the customer gets confused by the similarity of the names.

For example, when a web site called www.radiff.com appeared, the owners of www.rediff.com went to the courts and the Mumbai high court ruled that the name www.radiff.com is confusingly similar to the better known www.rediff.com and has to be withdrawn. Similarly, owners of yahoo.com won a case in the Delhi high court against the registrants of www.yahooindia.com. There are innumerable such cases around the world forming one type of domain name disputes.

The second type of disputes arise when a some body owns a trade mark in the real world and some body else registers a domain

name either exactly similar to the trade mark name or confusingly similar to it.

In such cases also the trade mark owners have been objecting to the use of domain names which are similar or confusingly similar to their trade mark name.

An example of this is the dispute between Maruti Udyog Ltd, the well known Car maker who took objection to a software company called Maruti Software Pvt Ltd, in Delhi on the domain name www.marutionline.com . The case was first decided in favour of Maruti Udyog in an international arbitration but later has been stayed by the Delhi high Court.

Disputes have been raised for using an Abbreviation of a Company name, (e.g.: objection by Volkswagen for the use of www.vw.com), Web Name extension (e.g.: objection by Yahoo for use of www.yahooindia.com), Brand Name Extension (e.g.: Ford objection for www.jaguarcenter.com) etc.

There are innumerable number of such disputes arising in the international markets every day.

Cyber Squatting

Some times when a person deliberately books a domain in a name which is popularly is associated with some body else, so as to sell it for profit to the same person, the act is called "Cyber Squatting".

In India there is no specific law in this regard. But many countries such as USA and Australia have enacted laws which essentially state that any registration of a domain in a popular name in bad faith, and for the purpose of making profit by a person other than

to whom the name is normally associated, is considered bad and can not only lead to the cancellation of the registration but also result in fine and imprisonment.

Popular companies such as Ford, Yahoo, Amazon etc as well as celebrity name owners such as Madonna, Harry Potter, Julia Robert etc have successfully evicted persons holding domain names which are derivations of these celebrity names.

UDRP

Currently, every domain name registrant is made to agree to a "Uniform Dispute Resolution Policy" (UDRP) with the registrar of domain names at the time of registration. As per this policy, any dispute arising out of the registration of the name is to be mandatorily resolved through an arbitration process with ICANN accredited arbitrators.

WIPO (World Intellectual Property Organization) has an arbitration center which is the most widely used arbitration center for the purpose. The arbitration process will receive the reference from one of the parties to the dispute and after giving due opportunity to the other party to present his case will adjudge on the dispute.

Normally the party having a registered trademark in any country will get a preference over another who may not have a registered trade mark.

Registration of Domain Names

In order to prevent large scale Cyber Squatting when a new TLD is registered, the registrars are now following certain pre-registration procedures to "Reserve" domain names to Trade Mark owners as a first option.

Accordingly, a certain period of say 30 days is allocated for initial registration of the new TLD only by the Trade Mark owners. Only after this period is over, the registration is thrown open to the general public.

This procedure is apparently a step towards avoiding a dispute on a later date. However, it is not certain that a Trade Mark owner cannot raise an objection even after failing to register his domain name in the allotted "Reserved Period".

Coexistence with Similar Domain Names

The system of linking the domain name with the trade mark has many weaknesses and has not been found effective in many cases.

The reason is that the Trade Mark system today allows the same name to be registered in different product categories and in different geographical areas. There is therefore a possibility that a Maruti Computers and Maruti Stationery may exist in India with registered trade marks in different product categories. Similarly a "Gem Granites" can exist in India as well as in South Africa in the same product category but in different jurisdictional areas.

Considering the impracticality associated with using Trade Mark as the predominant determinant of domain name rights, Naavi has developed a service called Verify For Lookalikes .The service, a prototype of which is available at http://www.verify4loookalikes.com is aimed at "Coexistence of Similar Looking Domain Names" and if accepted by the community would go a long way in reducing the incidence of domain name disputes.

Multilingual domain names.

Since the beginning of the Internet, the domain name system (DNS) had only allowed Internet addresses based on English characters. With the growth of Internet beyond USA, onto China, Korea and Japan, research has now shown that by 2005 only one-third of users will use English for online communication.

It has therefore been recognized that there is a need for introducing "Multi Lingual Domain Names". Accordingly, ASCII-encoded multilingual domain names using the Registry Registrar Protocol (RRP) has been introduced on an experimental basis. Now Multilingual domain names can be registered as second level domains under .com, .net or .org.

Apart from Chinese, Korean, Japanese, Greek, Turkish and many East European languages, domain names in eight Indian languages including Hindi, Tamil, Kannada, Telugu, are presently available.

While this development is welcome for popularizing the use of Internet, this gives raise to further complications in the legality of using Trade Mark related words in domain names. With the multi lingual domain names, it is not only the spelling that becomes a contentious issue but also the phonetic pronunciation of a trademark would also be a matter of dispute.

One example of the taste of things to come is that a Tamil site equivalent to www.kanthi.com would phonetically clash with another site of the name www.gandhi.com because the pronunciation of the words "kanthi" and "Gandhi" in Tamil are interchangeable.

Another example of a conflict would be when the meaning of a language name clashes with an English word of a different meaning. For example an equivalent of www.amla.com in Kannada may actually mean www.acid.com in English where as it may mean www.avocado.com in Hindi.

The domain name disputes based on trade mark rights will therefore become infinitely more complicated than what they are today making the need for a service such as Verify For Look Alikes, imperative.

After Maruti, it's Bharti

In a recent order of the Delhi High Court, an individual Vijay Kumar Bharti has been prevented from using a domain name registered by him as www.bharti.com and the rights to use www.bharti.com and www.bharti.net has been transferred to the Company Bharti Televentures Ltd.

The main consideration appears to be the similarity of the domain name to the name of the Company and the Company's desire to use the domain name space even though it had not been alert enough to register the name earlier.

It is not clear whether it was established that Mr Bharti had tried to pass off his site as belonging to the group or tried to take advantage of the similarity in name in any manner detrimental to the interests of the Company.

It is also not clear if the Court had been satisfactorily clarified why the Company could not use any alternative domain names including www.bharti.co.in as its business website or www.bhartiteleventures.com or www.bhartiteleventuresltd.com which would have provided enough scope for the company to carry on its business without unfairly restricting an individual from registering his personal name as a domain name and his fundamental right to carry on business.

The interim order has once again highlighted the growing influence of Trade Mark owners of the Meta Society over Netizens. The order gives a new meaning to the rights of individuals and makes them subordinate to the rights of a Company.

Just as in the case of Maruti Udyog's claim on the word Maruti, Bharti Televentures claim on the word "Bharti" impinges on the rights of many ventures and trade marks already using either "Bharti" or "Bharati".

Now one entrepreneur seems to have been provided an exclusive right over the name "Bharti" over all others including persons with the name Bharti and who have also been first to register the name on the domain space.

Perhaps both Mr Bharti and the Company Bharti can be mandated to use a service of the type offered by www.verify4lookalikes.com and live peacefully rather than fight.

"Copyright" has been a law which has evolved mainly for the protection of the rights of an "Author" of a "Literary work". Over a period of time, the scope and definition of the words "Author" and "Literary work" has expanded and extended beyond the paper world.

Objective

The object of Copyright law has been to encourage authors, composers and artists who create original works by rewarding them by grant of an exclusive right for a limited period to enable exploitation for monetary gain.

Copyright Law provides an "Exclusive" right to the "Author" to do or authorize the doing of any of the following acts in respect of his work or any substantial part thereof.

1. To reproduce the work in any material form, copying, printing, distributing, etc .
2. To reproduce and make adaptations of the work
3. To hire or sell the work or part there of

Whenever the "Right" of the author has been used by another in a manner which is inconsistent with the Owner's right, the Copyright is said to have been infringed. Using a Copyrighted material without the permission of the owner or in violation of the terms of license if any, amounts to infringement. In assessing an infringement of Copyright, there are two important angles to

be assessed. One is -Whether the usage falls under the category of "Fair Use" and the other is whether there was a "Permission" to use. In either case there is no infringement.

Fair Use

According to the doctrine of "Fair Use", Copyright is not violated by certain kinds of uses of the material which can be classified as "Fair Use". What is "Fair Use" is however a matter of case to case interpretation. The following acts normally are considered fair use.

1. Fair dealing of a work for private use including research.
2. Making copies of a Computer programme as a back up or for a purely temporary protection against loss or destruction or damage in order to use the programme only for the purpose it was supplied.
3. Doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer programme with other programmes by a lawful possessor. (E.g.: A programme developer who is trying to build compatibility with an operating system).
4. Reproduction by a teacher in the course of teaching
5. Reproduction for comments, parody, news-reporting etc to the extent reasonably necessary.
6. "Facts" and "Ideas" in any work are not subject to Copyright and their reproduction is not considered a violation of Copyright. However the expression and structure of any presentation can be subject to Copyright.

Fair use should be a short excerpt and always attributed. It should not harm the commercial value of the work -- in the sense of people no longer needing to buy it. Hence reproduction of the entire work is generally forbidden.

"Not charging" is not a criterion to determine "Fair Use". Hence, copying and reproducing work could be considered an infringement even if it is not commercially exploited.

Indian Copyright Act 1957

In India, copyright law is determined by the Indian copyright Act 1957 amended from time to time . Even though the Act was originally for non computer related work, through amendments in 1997, Computer generated works were brought within the purview of the Act.

It is important to note that Copyright becomes available to the author as soon as a literary work is created. It does not need registration even though Copyright can be specifically registered. Similarly, there is no need for a notice to be given for making copyright effective. Because of these two factors any web site document automatically qualifies for Copyright protection in favour of the author who wrote the contents of the web page. Any unauthorized copying of the writings or image from a web site therefore becomes a violation of the provisions of Copyright.

Copyright Protection on Web Pages

Some of the web page creators take specific care to not only display the notice of copyright on the site, but also use technical devices such as disabling the mouse right click. This puts a simple barrier preventing easy copying of content or images.

Some creators of images embed a water mark on images through a process called steganography to trace the picture that is copied. (Such steganographic technology has also been used by terrorists to exchange confidential text messages concealed within innocuous looking images.

Infringement of Copyright as per the Copyright Act could lead to both civil liabilities as well as criminal prosecution with a possible imprisonment of up to 3 years.

In USA, a separate Act called DMCA (Digital Millennium Copyright Act) has been enacted to cover Computer generated and Internet related copyright which among other things renders development of software or other tools which is substantially used for infringing Copyright as also a punishable offence.

In a well reported case in USA, a Russian programmer named Dmitry Skylarov was arrested while on a visit to USA for having developed a software that could convert Adobe E-Book files into a different format from which it could be easily copied.

Action was also brought on a company called Napster for making available a "File Sharing Technology" that enabled internet users to swap music files from one computer to another.

Several other countries such as South Africa have adopted or are in the process of adopting similar provisions to make developing and marketing of circumvention tools a punishable offence.

There has also been a significant outrage in the Community that the DMCA prevents technological research and innovation.

ITA-2000 and Copyright

As has already been mentioned in the earlier chapter, ITA-2000 was not intended to provide "Copyright protection to Cyber documents. However, the extension of "Any law which requires a document to be in writing" to "Electronic Documents" (Sec 4) does have the effect of making ITA-2000 applicable for Copyright on Electronic Documents.

The use of the word "Copies" in Section 43 (b) has been interpreted by some analysts as referring to Copyright Law. However the context in which the word is used provides a different meaning as an issue between the "Copier" and the "Owner of the System" and not the owner of the Copyright.

Fair Use of Copyright in Education- An Analysis

A huge debate is raging across the world on the meaning of "Fair use" of Copyright in the context of "Education". Chennai High Court some time back was in a position to contribute to this debate and make a mark in the history of evolution Copyright Laws in the global scenario when it took up for debate the Oracle Corporation Vs Radiant Software case in the beginning of 2001. (Ed: The case was later settled out of court)

Long before the current controversy in India, the following statement was made by a group of Chief Executives of the California State University (CSU), the State University of New York (SUNY), and the City University of New York (CUNY) in an effort to protect the Educational system from the onslaught of overzealous Copyright protectors.

Quote:

> "The fundamental mission of higher education is to advance and disseminate knowledge. This mission is realized through the use of various information formats, learning environments, and modes of delivery without unreasonable copyright restrictions."

Unquote :

In defining the objective of "Copyright Protection", the US Constitution states

Quote :

> [The Congress shall have power] "To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries;"

Unquote

Thus the fundamental raison d'etre for the existence of "Copyright Laws" is the "Promotion of Progress in Science". It is in this context that the role of "Education" comes to the fore as the main tool of the society to promote the progress of science

and arts. It is in recognition of this role of education that "Copyright Laws" have always treated "Education" as a special category of usage and provided for certain special provisions.
Some of these provisions are already enshrined in the statute itself while the "Doctrine of Fair Use" further adds to the explicit provisions.

Section 107 of the Copyright Act of 1976. (USA) explains the term of fair use thus :

> "Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified in that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. "

In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include –

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

2. the nature of the copyrighted work

3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole and

4. the effect of the use upon the potential market for or value of the copyrighted work

.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

Indian Copyright Act 1957 states under Sec 52 (1)(aa) as follows:

> (1) The following acts shall not constitute an infringement of copyright , namely:-
> (aa) the making of copies or adaptation of a computer programme by a lawful possessor of a copy of such computer programme, from such copy-
>
> > (i) in order to utilize the Computer programme for the purpose it was supplied or .
> > (ii) to make back up copies …
>
> (ab)….(Ed: Not reproduced here) .
> (ac) the observation, study or test of the functioning of the computer programme in order to determine the ideas and principles which underline any elements of the programme while performing such acts necessary for the functions for which the computer programme was supplied.

While referring to the use of Copyright material for the purpose of education, Indian Copyright Act 1957 states as under:

> Sec (1) [An Act does not constitute an infringement]..
>
> (h) the reproduction of a literary, dramatic, musical or artistic work-
>
> > (i) by a teacher or a pupil in the course of instruction; or
> > (ii) as part of the questions to be answered in an examination; or
> > (iii) in answers to such questions
>
> (i) the performance in the course of the activities of an educational institution, of a literary, dramatic or musical work by the staff and the students of the institution, or of a cinematography film or a record, if the audience is limited to such staff and the students, the parents and guardians of the students and persons directly connected with the activities of the institution..

It may be noted that the subsections (h) and (i) do not speak of software. Does it mean that this exemption is not available for software?.. This would be an unreasonable inference. What is more reasonable is that since the original act was not meant for

"Software" and the amendments were introduced to include "Software", some portions of the act may not be accurately reflecting the real intentions of the law in respect of software.

It is also true that the main purpose of passing these amendments were to prevent "Duplication" of "Software" for "Sale" to prevent "Piracy". In view of this, other cases such as "Educational Use" inter-alia involving "copying" was not specifically covered by the law.

If we consider that by the nature of the amendments brought in, it was the intention of the law makers to include "Software" as one of the objects of "Copyright Protection", (This is also corroborated by the sections such as 63B), the "Fair Dealing Concept" should be extended to software also.

Even if we consider that the provisions are vague or insufficient, the "Concept of Fair Dealing" is still applicable.

The Digital Millennium Act passed in USA specifically to cover the Copyright issues of Software has also provided specific exemptions for educational institutions to some extent. It states as under:

> EXEMPTION FOR NONPROFIT LIBRARIES, ARCHIVES, AND EDUCATIONAL INSTITUTIONS-
>
> (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph--
>
> (A) may not be retained longer than necessary to make such good faith determination; and .
> (B) may not be used for any other purpose.

In interpreting the above provisions we need to consider the following:

1. A Book may be used in teaching by the teacher. While doing so, he may reproduce the book in part or full to help him teach the contents. This is a "Fair Use". It is only if the copy of the book is sold for a separate consideration that the case of "Infringement for commercial gain" arises.

2. If the teacher charges a fee for teaching a copyrighted work, the fees does not belong to the author of the work. It belongs to the teacher for the value addition that he brings. There cannot be a royalty on the income of the teacher.

3. In the case of use of software by educational institutions, we must recognize that the usage of the software is of two types.

(a) The teacher or the educational institution may use the software for his/its own business. For example, they may use "Word" software for writing letters of the college.
(b) On the other hand, the "Word" software may also be used to teach students of "How to Use Word".

The provisions of the Digital Millennium Act as well as the amendments of the Copyright Act in India apply more appropriately to the "Own Use" of the software and "Reproduction for Sale" during the conduct of an educational programme.

In the Copyright world it is believed that infringement does not depend on whether the "Alleged Infringer" charged money or distributed the copy freely. It is the purpose for which a copy was distributed and its effect on the original owner that should determine the infringement.

In the case of training of an application software, there is no distribution of software. If copies were made during the training process, it would be to facilitate training since a software cannot be seen but has to be "Experienced" to understand how it works. Sec 5(1) (i) of the Indian Copyright Act is clear that a piece of art can be performed in front of the students and related audience without constituting infringement. Since a software can only be made to "perform" by loading it on the Computer, it may be argued that the loading of copies of the software in different machines in a training establishment does not constitute infringement.

If the loaded software were to be used to keep the corporate information of the institution, then there may be a need for a license.

Another aspect we need to consider is that whether the Copyright owner has lost any remuneration by virtue of the training institution using the software. If a training institute is teaching say "Photoshop", the trainees can make use of the software only on a machine where the software is "Licensed for use". Hence the training does not affect the sale of the original software but actually promotes it.

The current argument of the software developers seems to indicate that they are not claiming the "Copyright" on the software. They are actually claiming a right of "Exclusive Training". It is like an author stating that his book can be taught only by him or his licensee. If Newton had said that his principles can be taught only by him and any body else teaching his principles have to pay a royalty to him, imagine what would have been the progress of science which the Copyright vows to promote.

It is the greed of the software developers that has made them claim the right to define a "user license" specifically for training purpose. No application software may be claimed to have been developed for the purpose of "Training". It is developed for the purpose of "Use in an application" and the Copyright can extend only to this basic purpose for which a software was created. If Copyright has to be extended to a "Training Software", then it has to be exclusively developed for that purpose only.

An example of such a software is a multimedia tutor with in built functional demo module of the software. Such a software can be said to have been developed only for the purpose of training and its usage for training can be copyrighted. In the case of any other software, the purpose for which it is developed and the obligation of the law to protect the legal rights of the author extends in principle only to its use as an "application" and not its use for training.

A software developer however has the right to run his own training institute and call it by any name including "Authorized Center". But he can only determine the "Authorization" in respect of what is within his own control say on recruiting the trained personnel or use of special training skills and tools. For example, one can say people trained in Microsoft approved colleges alone will be employed by Microsoft. Beyond this the "Authorized Center" does not have a meaning. .

.

The next question we can examine is whether we need to distinguish an educational institution such as an "University" from companies such as "NIIT". The "Non Commercial Exploitation Clause" in the Copyright act is some times wrongly applied to understand that the concessions meant for "Educational Institutions" are not applicable for corporate training institutes.

However this appears to be a restricted view not in consonance with the spirit of the Copyright law. Today, there are no pure philanthropic educational institutions. Every institution charges a fee for imparting or selling education. Some may charge in thousands and some in lakhs. There are many higher learning institutions in India and abroad which charge up to Rs 10 lakh for a two year MBA programme. They do not become a commercial institution just for the reason of such fees.

Weighing all the aspects of the law as they exist and the principles behind them, it therefore appears that there is no "Copyright Infringement" when a software is used in training. There will be infringement only if copies of the software are distributed as Course material.

In protecting Intellectual Property Rights, Patents play an important complimentary role to Copyrights.

What is Patent Right?

"Patent" is a right given to an "Inventor" of a "Novel" and "Unobvious" device, "Useful" to the society, for exclusive exploitation for a certain period.

Product and Process Patents

"Patent" for an engineering product is granted for a "Product" and not just for an "Idea". Here the "product" which is an embodiment of "Design", and "Composition" and which expresses a functional property which has the usefulness and novelty, is the subject matter of Patent. Such patents are called "Product Patents".

In Pharmaceutical Patents, or when the product is a creation of a "Chemical Process", there is no physical form of the end product that provides the novelty. The underlying composition itself is the reason for the property of the end product and hence the process becomes a critical knowledge to be protected. This is the additional category of patent that is called the "Process Patent".

While the "Product Patent" protects the right on the identifiable end-product, the "Process Patent" protects the means of producing the product. This means that if an inventor has a patent on a process, his rights are limited to that particular process he cannot prevent the same product being manufactured by an alternate process.

On the other hand, if the patent is for the "Chemical" or the "Molecule" that has been invented by an inventor, then irrespective of the process, the end product itself is protected. Thus the "product Patent" in the pharmaceutical sector is the more powerful right than the process patent.

Nature of Software Patents

A Software product has a "Source Code" document and a "Functional Feature". The source code document is like a process of achieving the functionality. However, the intellectual property on this source code document is covered under "Copyright" and not under "Patent". Accordingly, even if a software code is copyrighted, if the same software functionality can be achieved by an alternate code, the copyright does not apply to the alternate code.

On the other hand, if a "functional feature" is patented, then it is protected against infringement from any alternate source code.

Normally, a software needs a "hardware" to show its functionality and usefulness. The device if otherwise novel, can be patented as an "Engineering Product". Just as a "Design" of an Engine which changes the functional properties, can be patented, the embedded "Software" which makes the hardware function in a useful and novel manner can also be patented. Such devices need not be classified as "Software Patents" even when the software is the main contributor to the novelty of the device.

A software per-se on the other hand is a virtual product and can be expressed only through a written source code or as a part of a hardware device. Since both these expressions are covered by the Intellectual property regime as either Copyright or Patent of the

device, there is a view that there is no need for the software to be separately patented.

Business Method Patent

With the advent of the Internet the scenario the software patent regime got further complicated since there could now be a "Software" which makes an "Internet Process" work in a novel way.

While software itself is a virtual product, a software working in a virtual environment is an even more abstract idea to comprehend for the purpose of granting a patent.

However, such devices that work on the Internet and produce a novel and useful functionality, are considered eligible for "Business Method Patent" under the US Patent rules.

Process of Patenting

While Copyright is an automatic right that arises as soon as a "Copyrightable Material" is created, Patent is a right that arises only upon "Registration" with the appropriate authority. In creating the Patent Rights therefore, the process of "Application" and "Approval" are very important.

The Patent process consists of the following steps.

1. Application by the Inventor to the relevant authority with relevant details of the subject matter of patent.

2. Examination of the application to find

    a. Whether the device is "Novel" and no "Prior Art" exists
    b. Whether the device is "Useful"
    c. Whether the device can be produced by any person with a reasonable knowledge in the subject with the details furnished by the inventor along with the application.

If after an examination the patent authority comes to the conclusion that the device is patentable, the patent would be suitably registered. The right then comes to existence for a stated period.

Jurisdiction of Patent

Patent being a creation of "Statute", it is a right restricted to the territorial jurisdiction of the granting authority. Thus a patent granted in USA is not necessarily applicable in India. However, the WTO regime through various mechanisms such as Patent Cooperation Treaty (PCT) is trying to make it simpler to make "Common Examinations" so that the "Procedure for obtaining a Patent" and "Determining the Priority" for the purpose of granting the patent would be easier in all countries who are part of the treaty.

Infringement

Infringement of a Patent consists of the unauthorized making, using, offering for sale or selling any patented invention during the term of the patent.

If a patent is infringed, the patentee may sue for relief in the appropriate court. The patentee may ask the court for an injunction to prevent the continuation of the infringement and may also ask the court for an award of damages because of the infringement.

Some of the famous Patent infringement disputes in the Cyber World are the "Amazon's Single Click Method of Online Buying,", "Price Line's Reverse Auction method", "Open market's E-Commerce Method", "British Telecom's Hyper Linking method" etc.

Status in India:

The status of software patent in India is hazy. The Patents (Second Amendment) 1999 Act which was passed by the Indian Parliament during May 2002 has given raise to a debate on whether software patents can now be patented in India.

According to the amended Section 3 of the Patent Act 1970, the list of non patentable items contain "..computer program per-se".

Some of the experts in the country feel that this is indicative of the legislative intent to make "Computer Programs" which have a technical contribution as patentable. This view is based on the European Union guideline of a similar nature.

Had this view been confirmed with a procedural guideline on how to apply for software patents, then the issue would stand clarified. It now appears that the relaxation is applicable only to facilitate patent for devices where the essential functional feature happens to be a software as in any electronic device with an embedded chip.

However, as a signatory to the PCT (Patent Cooperation Treaty), Patent applications can be made in India even for software and Business method Patents under PCT. The examination may however be taken up in any of the foreign centers such as USA or Europe.

The consequences of Patent infringement is mostly felt by the Web site owners and software developers rather than the common Netizen who browse through the websites. Companies who invest substantial amounts in the development of virtual assets should however be careful not to be pulled up for infringement by an international patent holder.

There is therefore an urgent need to bring software and business method patents of web utilities under Indian patent system with the proviso for compulsory licensing.

If such a provision is available in the Indian statute, then it may be possible for Indians to be protected against infringement regarding basic devices software/web utility devices such as "Hyper Linking", "E-Commerce" etc.

Provisional Patent

USPTO (United States Patent and Trade mark Office) has made available a system of "Provisional Patent" for the assistance of Inventors".

Under this process, a simple procedure is made available to the inventor to register a "Patent Document". The inventor is then given 12 months time to file a formal patent application with all the relevant details. However, if there is any parallel development of a similar device, the date of priority to determine who would

get the credit for "Prior Art" would be determined with reference to the date of registration of the provisional patent.

More over this enables protection of the Inventor from other predators during the time the "Invention" is under consideration of the patent authority or when the inventor is sharing the knowledge with other persons who are engaged in developing the device for final patent application.

This provisional patent system is open to Indians also. However the provisional patent does not create the patent right as such and is only a recognition that the inventor will get priority over any other person coming up with the same idea later.

CHAPTER XI

NETWORK SERVICE PROVIDERS

Internet is a vast library of electronic documents made accessible through a network of Computers. In this process of making it possible for a Netizen to access Electronic Documents, several technical intermediaries play significant roles.

The Netizen uses a modem or a direct cable to first connect his computer to the nearest Internet Service Provider (ISP). He types the domain name of the site that he needs to visit on his browser. The ISP then takes him to a Domain Name Server which resolves the domain name to the corresponding IP address and connects him to the host computer. Some times, the Domain Name Server used by the ISP may not be able to track the IP address. He then directs the query to one of the other Domain Name Server in the global network until the IP address is located. The ISP is therefore providing a Domain Name Resolution service and the International Connectivity service.

The web site itself is a bunch of electronic documents residing in a Computer which is having a specific IP address for identification and always remains connected to the Internet backbone. The web site owner uses the services of an intermediary who provides a facility to host the web site and maintain its connectivity to the Internet.

Most ISP s also provide E-Mail facility by providing a mail box for incoming e-mails (POP3 Service) and a facility for sending e-mails (SMTP Service) from the client's computer to any other computer in the Cyber space.

Additionally, many web sites themselves offer services as an intermediary between the Netizen and the ultimate service provider. For example, a portal may provide a "Search" service or an "Online Credit Card Authentication Service".

There are also sites which offer "Document Format Conversion Services", "Web Graphic Services" etc.

Some also maintain sophisticated software and provide its use to customers on a "Pay as you use" basis. These service providers called Application Service Providers (ASP) are also essentially intermediaries.

Thus in the Cyber Space, there are many hardware and software intermediaries between the ultimate consumer and ultimate service provider.

Cyber Cafe

In the array of services provided by intermediaries, there is also another important service which is very critical for countries like India. This is the service of providing Computer, Modem and Connectivity to the nearest ISP on a rental basis. These Internet Access centers have come to be called as "Cyber Café's" and are important intermediaries making Internet access affordable to common people.

Just as the STD booths provide telephone service to those who do not have phones at home, Cyber Cafes provide internet access without the need to invest in a Computer and an Internet account. It is also useful for a traveling Netizen for accessing his web based e-mail or for surfing the web when he is out of his place of residence.

While Cyber Café's have a number of Computers, there is also a service of providing single Internet access devices at public places called "Internet Kiosks". Such devices are in the priority planning of the Governments to make Internet accessible to small towns and Villages as a means to reduce the ill effects of "Digital Divide" caused by the concentration of information power with the Internet users.

With the presence of such a variety of intermediaries, quite often, Cyber Crimes get committed with the use of resources provided by an intermediary. In such cases it would be necessary to determine the vicarious responsibility of the intermediary.

The Information Technology Act-2000 addresses the issues of both releasing the intermediaries from being held responsible for crimes committed by their service users as also fixing accountability for them to assist the law enforcement when required.

Liabilities of a Network Service Provider

According to Section 79 of the ITA-2000, no person providing any service as a Network Service Provider is liable under this Act, 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 due diligence to prevent the commission of such offence or contravention.

For the purposes of this section, Network Service Provider means an intermediary and "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.

"Third Party Information" means any information dealt with by a network service provider in his capacity as an intermediary.

The definition of the "Intermediary" given above Section 2 (w) is very important to determine the legal liabilities of an ISP or a Cyber Café. With respect to any Cyber Crime that is committed.

The Cyber Café can be effectively brought under the definition of "Providing Any Service with Respect to an Electronic message".

In order that the intermediary of an Internet service escape legal liability, he should have "No Knowledge" of the crime and that he should have exercised "Due Diligence". The "Due Diligence" is an aspect which is to be benchmarked to the expected level of prudence that the Cyber Café owner is expected to exhibit.

Section 65 of the ITA-2000 on the other hand imposes certain responsibilities on an ISP for preserving evidence in respect of any Cyber Crime.

This important section states that

> "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."

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.

This section clearly lays down that the person responsible for maintaining records generated in a Computer has a responsibility to keep the records safe "when the computer source code is required to be kept or maintained by law for the time being in force".

The term "Source Code" mentioned here covers inter-alia, all "Server Logs" that record the happenings in a Computer system. Even though there may be some doubt as to the applicability of the term "Source Code" to server log records, the context in which the term has been used as well as the fact that the header information of a mail is a "Computer Command generated by the e-mail programme", and the server log record is a "list of such commands" indicate that any such records will be covered under the definition .

One of the critical areas where the ISP s such as VSNL, Satyam, Dishnet and others would be questioned is in regard to the "E-Mail" data. As from October 17, 2000, every e-mail sent and received by any person in India is an electronic record that can be produced as evidence in a court of law.

Even though it is possible to produce a print copy of an e-mail as proof of evidence, the better option would be to produce the "Message ID", the "Arrival time of an incoming mail" or "Leaving time of an outgoing mail" as supporting evidences to the claim of having received or sent an e-mail. The time of entry and exit of the message is also relevant for determining the contractual effect of the message. The IP address of a Computer which originates a message or is the destination of a is also an important contractual information that is useful to prove a contractual message..

Normally every ISP automatically captures the above data in their server logs. If required the ISP can be maintain a backup of this data also. When called upon by a Court to produce, this record can be produced by the ISPs. Just as in the case of a "Registered Post" the post office can give evidence whether a particular letter was sent/received or not sent/received, even though it cannot certify the contents, the ISP can certify whether a message was sent/received or not. This would be a very powerful secondary evidence of the message itself even though the ISP cannot certify the contents.

At present the Government has not notified the "Time" up to which such records are to be maintained. Some ISP s keep records of "Access" containing the log in ID, the telephone number from which a dial up account is accessed and the allocated IP address of the user machine. The information on the messages themselves are not however systematically stored. They are often over written by the system like cache records. In major ISPs the records may get erased within a week to 10 days.

It is interesting to note that the European Home Office has proposed that ISPs and other network operators retain data on telecommunications usage, such as records of e-mail and Internet use, for seven years. This is an important notification due from the Government of India in respect of ITA-2000. In the absence of a notification, ISP s will be required to keep the records for a "Reasonable Time" and what is a "Reasonable Time" is left to the interpretation of the Courts.

Considering the norms set by the European Home office as well as our own norms in respect of Bankers Books Evidence Act, as well as the slow judicial process in India, ISP s must be prepared to look at keeping the records for a "Reasonable Time" of up to 7 years.

Simultaneously, ISP s must also be prepared to keep the records permanently at the request of their customers, failing which they may be accused of knowingly destroying the evidence.

Role of Cyber Cafes redefined

While ITA-2000 has defined "Network Service Providers" and their liabilities which as we have seen above could be inclusive of the Cyber Café's also, there has been an attempt to give a definition for Cyber Café separately by the law enforcement agencies.

The guidelines for Cyber Cafes, proposed by the Mumbai Police is one such important piece of quasi legislation which actually should have been a part of the ITA-2000 rather than a guideline from the Police department..

According to the suggested guidelines, Cyber Café's will be defined as a place of public amusement under Section 2(9) of the Bombay Police Act, 1951 and will be regulated accordingly.

If this definition becomes a universal norm, then Cyber Café's will be subjected to the same rules and regulations that apply to Cabaret Centers. The fact that Internet is only an enabling tool and a visitor to a Cyber café can visit not only an "Amusement Site" but also the "Tirupati Temple Site" or a "Net Varsity Site" or the "Ministry of Information Technology Site", is lost sight of by the proposed guidelines planned to be issued by the Mumbai Police.

The Cases of Rediff.com and TOI

The role of search engines came to be questioned in a case heard by the Pune High Court against the well known Indian portal Rediff.com. In this case, it was alleged that Rediff.com was providing a search service on their web site where a person can search for and obtain hyperlinks to pornographic sites and hence the company is punishable under Indian Penal Code for distribution of pornographic material. The court actually issued notices and summoned the directors of the Company.

A similar case was also filed against Times Of India when it was found that one of the free web pages hosted by the company for a member of public contained pornographic material.

Section 79 of the ITA 2000 provides direct confirmation that TOI would be protected against being held responsible for publishing of pornographic material on its server from one of its customers provided they can prove in their defense that they were ignorant of the fact and had taken all reasonable care to prevent the same.

However the case of Rediff.com needs to be looked at from the angle of whether the search engine service falls under the category of "Intermediary" services or not. Even though the Act may not be very specific on this aspect, the nature of search engine service as an aid to the common Netizen to find information on the web cannot but be held as a service of the "Intermediary". This is so because, it is inconceivable that any Netizen can today surf around without the assistance of a Search Engine.

One of the points which has come up for discussion during this case is whether it should be made mandatory for search engines to filter adult sites from the output. Even without any legislative compulsion some of the search engines are now making such provisions.

The need to declare "Search Engine" as a "Community Service" under law, is also important since there are several other aspects of their functioning that would come to be questioned if they are not adequately protected. For example, the search engines can be accused of bias and fraud by manipulating their results if the ranking of sites is proved to be inefficient.

Similarly, since the search engines need to enter and search web pages for "Key words" and "Meta tags", there is also the possibility of accusation of "Unauthorized Entry".

To prevent such dubious claims, it is better if search engine services are declared as "Intermediary Services" and are provided a reasonable protection against the limitations of technology.

The Role of Call Centers

The IT enabled services such as Call Centers provide some information to the public often through electronic documents (When the Call centers function through online Chat modes). It is debatable if their services will also come under the definition of "Intermediaries" since they form part of the chain where information is provided from a Company to its Customers.

The Role of Medical Transcription Centers

The Medical Transcription centers receive electronic files in one format which are converted to electronic documents in another format. In a way this is also an intermediary service where electronic documents are created and redistributed with value addition. Here the intermediary is exposed to the risk of inefficient conversion leading to legal liabilities. There is also a "Data Confidentiality Loss" risk which can make the transcription center liable.

In some countries "Data Protection Laws" have been enacted to provide legal remedy to the affected parties on account of inefficient handling of sensitive data by data intermediaries.

Since India is yet to pass any laws regarding the same, it may be debated whether such "Info-mediaries" can be called "Network Service providers" under Section 79 and made accountable for due diligence or they should be left to sort out the inter-se liabilities with their principals under the normal Contractual obligations.

Can ISP 's lock Away Mails?

In the Go2nextjob.com case in New Delhi, two of the directors of the web hosting firm which stopped the services to a client allegedly having defaulted in the payment were arrested and accused of "Hacking". This opens up a discussion on the remedies available to an ISP providing e-mail services in case of a non payment of charges.

- One obvious remedy is to close the e-mail box so that future mails are not received and they bounce back.

- Second remedy is to close the e-mail box for access even to the account holder so that the mails already in there or those which are allowed in are kept under lien.

- Third remedy is to penalize the account holder in financial terms and allow the service with a penal charge.

The issue has to be discussed both from the legal as well as practical points of view. It must be admitted that it is impractical for the ISP to expect collection of penal charges for the delivery of e-mails beyond the expiry of the account period since the root cause of discontinuance is the non payment of the fees in the first place.

Bouncing back may be an acceptable solution since the sender at least has the option to re-send the mail to any other address of the recipient.

However it is not a preferred solution if we agree that e-mail is a critical service and "Bouncing" which can occur even when there is no default in payment (e.g.: E-mail box full) places the sender and the addressee at a serious legal disadvantage.

Sending a communication to an alternate address of the addressee about the bouncing of e-mail in the designated e-mail box may be a choice for ISP s to consider so that the addressee is held accountable for keeping his e-mail box in serviceable condition.

The withholding of access of the mail box and trapping the incoming mails in such a box means that the sender is not aware that the box is not accessible to the addressee and the delivery may come under dispute at a later day.

If the addressee chooses not to renew the account at all, then the mails may be permanently lost.

There are issues of privacy as well.

However in terms of the legal implications, the ISP may be able to establish that he has a lien against the property (E-Mail which is an electronic document belonging to the e-mail box owner) which has come into his hands in the normal course of business for the dues directly connected with the provision of the service.

Though legally sustainable, this option is extremely customer unfriendly and is better avoided.

The solution to this day to day problem of the Netizens lies in the acceptance that the Netizens should have a reasonable option to change their service providers when required. The following suggestion is therefore placed before the public which can be voluntarily imposed by ISP s themselves or by a suitable amendment to the law itself.

Suggestion:

In order to face situations of non payment as well as the non availability of space in the box, it must be made mandatory for the ISP to provide an option to the account holder that "In the event of the e-mail box being full or otherwise the service is to be discontinued, all incoming mails are to be diverted to an alternate e-mail address to be provided by the addressee along with a notice to the sender of the fact that the mail has been diverted. (Without assigning any defamatory reason thereof).

This facility may be continued at least for a period of six months from the date of discontinuance.

A similar "Redirection Service" may be provided by the web hosting persons as well. (to prevent cases similar to go2nextjob.com).

We may observe that there are similar provisions for "Notice of Discontinuance" for Certifying authorities under the ITA-2000 and similar laws around the world.

It is therefore possible to incorporate similar notice period for discontinuance of any e-mail or web-hosting service as a part of the ITA-2000 itself or as a part of the ISP guidelines.

This will ensure that no critical service such as an e-mail service or web hosting would be discontinued unless there is an adequate notice and diversion of visitors to an alternate address.

CHAPTER XII

PRIVACY AND PERSONAL RIGHTS

Amongst the personal rights which a Citizen in a Democracy enjoys, "Right to Privacy" and "Right to Freedom of Speech" are the very important. These rights are the foundation of democracy.

In the context of the Cyber Space, the civilized world expects that a similar right is available for the Netizens also.

As long as Netizens do not enjoy a separate legal status as "Citizens of the Cyber World", they are bound by the laws of the land to which they are attached by virtue of their citizenship or physical presence.

If in a future scenario, there is a system of Cyber Democracy where the Netizens vote and elect their leaders and develop a Governance system independent of the physical nations to which they otherwise belong, the laws of privacy and freedom of speech could be drawn up separately for the Netizens.

Until such time, we live with the current country specific laws along with the conflicts they generate when people meet in the Cyber space.

Hence an American Citizen will enjoy his Meta society rights as an American Citizen even as a Netizen. On the other hand, an Indian Citizen will be eligible for the rights available to him in the Meta Society even when he is a Neizen. Thus different members of the Cyber society enjoy different personal rights even though Cyber society itself is a borderless community which qualifies to be called a nation by itself.

TYPES OF PRIVACY

Right to Privacy has two dimensions. One is that a person should have a choice of determining how much information about him can be shared with the society. The other is, how much of freedom others have to intrude on his time and space.

For example, an individual may not like his/her age to be known to every body else. More seriously, he/she would be very sensitive about information such as his/her "Medical History" or "Financial History".

On the other hand, the society may like to know whether the person has any communicable disease or is a bad credit risk.

It is therefore a matter of a mutual settlement between an individual and the society that determines how much of "Privacy" is reasonable.

Apart from the individual's sensitivity for some of his personal information, Privacy is also important to prevent unscrupulous persons from using the information to commit frauds or other crimes.

CYBER STALKING

The Internet Technology provides an easy technical means of following an individual when he surfs different web sites. This tracking can provide very useful information to any intelligent marketing agency to understand the potential buyer's preferences. This could help them provide customized services to the buyer during his subsequent visits. Obviously, such

personalization actually helps the buyer in his process of decision making and he may not therefore mind the tracking of their buying habits.

But some consider this stalking an annoying intrusion of their privacy. For example, a person who is browsing through pornographic sites may not want to be embarrassed with a mail that sends a special offer in a related field. Similarly, an employee browsing through job sites may find it embarrassing if he knows that some body is watching his movements.

Cyber stalking of children who form a significant number of Netizen community is an area of special concern since they may lack the capability to defend themselves in case the information extracted from them online is used against them in the Real world. Children are also often used for extracting sensitive information about their parents which may later be used for committing frauds.

Cyber stalking is therefore considered objectionable by most countries.

India doesn't have any specific legislation for Cyber stalking at present.

COOKIES

Placing "Cookies" is a popular means by which website owners gather information about Netizens. Basically, Cookie is a "tag" which identifies the Computer from which a site is accessed. It doesn't alter any other functioning of the computer and is passive "Identifier Tag".

The server hosting the web site keeps the data of how many times the site was accessed from the computer which had the cookie and what were the activities of the browser at the site during the session. The Cookie is a "Blind Identifier" and has no link to the "Real World Data" of the person who is tagged. To that extent Cookie by itself cannot be used to identify a person in the real world.

Only when a Computer user fills in an "online form" with personal information, he would be exposed to the risk of his Cookie being used as a handle with which his personal information can be accessed.

Cookies on the other hand serve many useful purposes such as "Customizing" information services, advertisements etc. Since an intelligent analysis of information gathered through Cookies can lead to the "Profiling" of the Netizen, the information has commercial value to the marketing person. Some Netizens therefore feel that unless their consent is obtained, such information should not be extracted. To that extent placement of Cookies is considered objectionable.

Cookies do not include executable programmes which some marketing persons prefer users to carry on their computer. For example, if you are using a "Free Internet Access Service", the service provider may want you to keep an "Adbar" or a "Customized Browser" on your computer. This is an executable programme.

It is often said that many programme vendors including Microsoft, embed programmes within the main software, whose purpose is to collect and forward valuable information about the user.

Even the hardware manufacturers like Intel have been accused in the past of collecting some information from user's computer without his knowledge.

Such devices are not to be confused with Cookies.

Further, all the major browsers provide an automatic facility to block the "Cookies" if required. "Cookies" therefore are on the user's computer mostly with his consent

Hence, even though a "Cookie" is often accused of being the prime Privacy invasion tool, its direct role in this regard is limited.

PRIVACY INVASION BY THE GOVERNMENT

Apart from the issue of marketing agencies collecting consumer information for commercial exploitation, the other important issue in Privacy is the right of the Government in collecting information about its Citizens. Even in the Real world, Governments are the largest repositories of personal information.

For example, the Tax department in any country has details of a Citizen's income, which even his spouse may not know. Since the Government and the Citizen have a mutually dependent and beneficial relationship, it is not possible to deny the Government the right to know some key personal information including his identity, age, income, presence of communicable deceases etc.

However, there are disagreements on whether the Government should know information such as Who are his friends? What does he do during his leisure time? Whether he visits a Porno site or an Education site on the Net? etc.

Similarly, when the issues such as Crimes and National Integrity come into play, conflicts arise between what are the rights of a single person vis-à-vis that of the society. Obviously, the interest of the society should be above that of a single person. The problem however is in exercising the judgment of whether something is or is not in the interest of the society. Concerns also arise whether the law enforcement authorities can use their powers with diligence. It is in these circumstances that the action of a Government some times is looked upon as excessive and unnecessary.

In the real world, every Government reserves the right to snoop on the Citizen's private mail or telephone calls or to undertake a search of your premises, or hold him in a lock up, if there is a reasonable ground to believe that he has violated or is likely to violate law. However, the law and the procedures for implementation will normally prescribe checks and balances within the system so that these emergency powers cannot be abused.

The problems on the Cyber world are different for several reasons. Firstly, it is far easier to snoop on Cyber activity than the real activity. It costs less and is certainly more efficient. It can also avoid giving any clue to the victim that his privacy is being violated. If therefore the Government wants to watch a Netizen's activity, it can do so effectively and in total stealth. Herein lies the danger of innocent persons being harassed as suspects of unintended and uncommitted crimes.

In USA, the FBI is trying to make it mandatory for all ISP s to install a software monitoring device called "Carnivore" so that the Internet data transfers can be monitored and filtered if required.

In India, the Indian Post office Act as well as the Telegraph Act permitted the Government to intercept private communications in times of public emergency. In an important judgment, the Supreme Court (People's Union of Civil Liberties Vs Union of India reported in AIR 1997 SC 568) stated that the substantive right to privacy includes telephone conversation in home or office.

Now the Information technology Act 2000 has vide sec 69 of the Act empowered the Controller to direct any agency for interception of an electronic message if it is in the interest of the Country's integrity and security. On the other hand, under Sec 72 of the Act ITA-2000 can impose a penalty on officials or Certifying Authorities who breach confidentiality of information that they come to handle while discharging their duties.

However, the Telecom guidelines for setting up of Submarine Cable Landing stations make it mandatory for the ISP s to set up hardware and software to enable the state to monitor and filter the Internet data traffic as per the requirements of the Government.

As already stated, Privacy Rights of an individual against the Government will always be a subset of the Rights that the Government provides to its Citizens and it will depend on whether we are dealing with a Democratic, Autocratic or a Military Government.

PRIVACY INVASION BY THE EMPLOYER

Another area of frequent dispute is the privacy of an employee as against his employers when he receives e-mails or surfs the web using his office computer. While the employer feels that since the

employee is using the office resources, everything that is within it, should also be within his right to see and monitor.

However, if this were so, then every letter the employee receives in the office address or the telephone call that comes to the office telephone will be within the right of the employee to snoop into. Obviously, the meta society has rejected the right of an employer to listen to the private telephone conversations of the employee or to see his private mails. Going by this precedence, the Cyber Society should also reject the employer's right on the monitoring of the Cyber activities of the employees.

The only way that an employer can have access to private electronic communications through the office resource is by separately entering into a contract with the employee that such a right exists. This may perhaps be part of the service rules.

In the absence of such express contract, no right over the Private information of the employee on the Computer should be implied.

This part of the law is yet to be established and there is scope for a counter argument.

ANONYMITY

Along with the Right to Privacy we also need to discuss the "Right to Anonymity" if such a right exists. The growth and popularity of Internet as a medium of communication owes in great measure to the "Anonymity" factor. If anonymity on the Net is killed, one of the great strengths of the Internet in cleansing the Corrupt part of the Meta world will be killed. It is the possibility of anonymous expression on the Internet that provides a big boost to Democracies of the world.

To an extent the "Right to Anonymity" is also linked to "Freedom of Speech". As long as Internet remained a means of communication, no body bothered much about the anonymity aspect. It was only when E-Commerce became an integral part of Internet usage that the need to have "Impeccable Identity" became paramount.

Governments are also wary of "Anonymity" as it could be exploited by criminals. Another reason why Governments would back full identity of all those who surf, would be to ensure maximum "Tax Collection". Hence, "Anonymity" would always result in a fight against authority.

In the meantime, in view of the popularity of "Anonymity", many service providers have emerged to protect anonymity in the Cyber world. They mask the IP address of the Web surfer and replace it with the service provider's address so that the visited website or intermediary sniffers will not be able to identify the original IP address. Similar anonymous services are also available for e-mails.

This conflict between encouraging anonymity and free expression as against protecting commercial transactions through impeccable identity, will long be debated.

PSEUDONOMITY

One of the midway solutions to resolve this conflict is to retain the best of both worlds by promoting "Pseudonymity".

Pseudonomity is where, the real identity is hidden and a "Screen Identity" is used for all Cyber activities. ISP s provide you an

opportunity to assume a pseudo name on the screen that can be traced back to the original person if need be.

As long as "Traceability" is thus ensured, the Government agencies may have no objection to let the Netizens enjoy the benefits of anonymity.

The ISP will however be bound in such cases by the duties thrust on him by the voluntary or legal adherence to a set of privacy protection norms.

PROTECTING PRIVACY

Apart from the services such as the anonymizer that protect a Netizen's identity, there are services that create decoy cookie records that can camouflage the identity of the Cyber traveler. Until Governments ban such services as they are trying to do in respect of "Devices that assist Copyright violations", they can be used effectively by Netizens who want to protect their Privacy.

Another option to protect privacy is to adopt "Encryption" of communication. Unfortunately, Government authorities have already moved in this area and made it mandatory that the encryption standards used are within their capability for decryption.

Indian authorities have made it mandatory in the ISP guidelines that they would ensure that transmissions are not encrypted beyond a permitted encryption level and that the users have to provide assistance in decryption by lodging the "Private Key" if required.

There is an anomalous situation in India regarding encryption of internet data since the ISP guidelines prohibit encryption of data beyond 40 bit level. However, most of the encryptions used by the browsers and e-mail clients during secure transactions use encryption of much higher level. In fact 40 bit encryption is considered too weak and its usage can very well be held as "negligence" in any analysis of security standards.

There appears to be a contradiction arising from the ITA-2000 itself since the rules for certifying authorities prescribe digital signature encryption standards which are 512 bit and above.

In the ISP guidelines, there is also a suggestion that the set of private keys are to be lodged with the regulatory authorities if encryption of higher level is to be used.

Similarly, there was a move in India of introducing a dual key system for digital signature where one set of public-private keys would be used for encryption and another for digital signature so that the private key used for encryption can be lodged with the Controller when necessary. These are however fraught with the risk of privacy invasion and hence are not considered prudent.

Another way of protecting "Privacy" is to develop an industry norm for "Acceptable Privacy Policies" to be adopted by web sites. There are many voluntary organizations such as TRUSTe who are emerging as reliable approval agencies and their seal of approval carries a value as to the integrity of a web site that the personal information would not be misused. Such organizations expect web sites to declare their Privacy Policy on the web site and adhere to them strictly. Approved sites will then be authorized to sport a logo of the certifying agency and many hard core Privacy conscious Netizens owe not to part with personal data unless such a certificate is available.

Platform for Privacy Preferences (P3P)

Another initiative that is being pursued by the Netizen community to protect online privacy is the development of P3P. a Platform for Privacy Preferences. This is protocol for sharing private information over the Internet which enables the browser to transparently transmit sensitive data such as a credit card number to a P3P-enabled Web site.

The Project, developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit.

At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users.

P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

Hackers and Privacy

Protection of data against hackers is not a “Privacy problem” per-se but is a different crime. This would require the use of use of technical defense systems such as firewalls both at ISP levels as well as personal computer level.

LAWS ON PROTECTION OF AN INDIVIDUAL'S RIGHT TO PRIVACY

Right to Privacy is a fundamental right of a human being. Most countries have included it in the rights guaranteed by the Constitution itself. International conventions on Human rights also include it as a fundamental right of a civilized society. The European Convention on Human Rights (Article 8), The Universal Declaration on Human Rights (Article 12) and the Treaty on Civil and Political Rights (Article 17) are a few of such conventions .

UN GUIDELINES FOR PRIVACY OF PERSONAL COMPUTER DATA

The United Nations General Assembly adopted a resolution on December 14, 1990 laying down guidelines concerning handling of computerized personal data files by member states.

While the procedures for implementing regulations in this regard were left to the initiatives of each state subject, certain principles concerning the minimum guarantees that should be provided in national legislations were spelt out in this document. These can be considered the building blocks for Privacy laws in any country.

The principles laid down by the UN resolution are,

1. Principle of Lawfulness and Fairness.

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. Principle of Accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. Principle of Purpose Specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, should be legitimate and when it is established, should receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

4. Principle of Interested Person Access

Everyone who offers proof of identity has the right to know whether information concerning him is being

processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and when it is being communicated, the particulars of addressees.

Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

4. Principle of Non Discrimination

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

5.Power to Make Exceptions.

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

6. Principle of Security

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

7. Supervision and Sanctions

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

8. Transborder Data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

9. Field of Application

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

10. Personal Data files kept by Government International Organizations

The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

Each organization should designate the authority statutorily

competent to supervise the observance of these guidelines.

12. Humanitarian Clause

A derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

A similar derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.

OECD GUIDELINES

The OECD (Organization for Economic Cooperation and Development) which is group of 30 member countries with a commitment to fostering good governance and market economy has taken some key initiatives in ensuring protection of Privacy of personal data of citizens in the member countries. This has immediate relevance to Netizens who claim the rights available to the respective member countries.

Apart from the European Union countries, USA, UK Canada, Australia, New Zealand, Japan, Korea, Mexico are some of the other countries who are members of the OECD. India has a cooperation program with OECD as a developing nation and is not a member of OECD.

OECD adopted a set of guidelines governing the protection of privacy and transborder flows of personal data on 23rd September 1980.

These guidelines recommended that:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines.
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth.
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

The principles of the OECD are:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used except:

a) with the consent of the data subject; or

b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

It may be noted that the guidelines also provide that member countries should take into consideration the implications for other Member countries of domestic processing and re-export of

personal data and should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

EU GUIDELINES ON DATA PROTECTION

Based on the OECD guidelines, the European Union has come out with its own directive on data protection applicable to its members.

Some of the salient features of the EU guidelines on data protection are given below.

The Directive requires EU member states to adopt national legislation ensuring a minimum level of protection to information by which individuals can be personally identified.

This includes not only information collected on-line, but information maintained on automated systems and some paper records.

The Directive limits data collection, processing, storage, and dissemination activities to the following.

- Information may be stored and used only for the purposes for which it is collected and must be maintained in a form that does not permit identification of individuals longer than necessary for those purposes.
- Information must be accurate, up-to-date, relevant, and not excessive in relation to the purpose for which it is stored.
- Information may be processed only with the individual's consent, when legally required, or to protect the public interest or the legitimate interests of a private party, except when those interests are outweighed by the individual's

interests.

Transfer of Information to Non-EU Countries

The EU guideline forbids the transfer of information collected in the EU to countries that lack "adequate" privacy protections. This is a source of particular concern to multinational companies operating outside Europe and Indian Companies providing backend data processing services.

EU authorities consider the U.S. to have inadequate privacy laws, at least for many categories of transactions.

The above restriction on transborder data flow is subject to some important exemptions. Most notably, transfers may be made to such countries if

- The individual consents "unambiguously" to the transfer.
- The transfer is necessary to perform a contract between the individual and the data controller (the entity with decision-making control over the use of the information), or is necessary to perform a contract between the data controller and a third party if the contract is in the individual's interest.
- The transfer is legally required or necessary to an important public interest, or is necessary to protect the individual's vital interests.
- The transfer is from a register accessible to the public or to any person who can establish a legitimate interest in consulting it.
- The transfer is authorized by an EU member state based on a showing that the information will be adequately

protected in the destination country. (Such protection may result from appropriate use of contract clauses.)

It appears that the directive is far harsher than what was envisaged in the OECD guideline particularly in respect of transborder flow of data to other countries who may not have data protection laws matching the EU directive.

PRIVACY LAWS IN USA

USA has not yet fully accepted the EU guideline on Data protection , but has various federal and state legislations that try to protect the privacy rights of the individuals.

In particular, the Electronic Communication Privacy Act (ECPA) specifically protects privacy of an individual in USA in online communications.

There are also specific laws for protecting Health data through HIPAA (Health, Insurance Portability and Accountability Act, for protecting financial data through Gramm Leach Bliley Act (GLBA) , for protecting children through Children Online Privacy Protection Act (COPPA)

Some of the salient features of the US legislations for protection of privacy are briefly discussed here.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 1986

The ECPA provides any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in

violation of the provisions of the Act may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

The USA Patriot Act passed immediately after the historical terrorist attack of September 11th 2001 on the World Trade Center has however brought in some changes to the ECPA.

Now a new voluntary disclosure exception for emergency situations has been added to the provisions. Under this exception, if a provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of certain information without delay, the provider may disclose that information (content or non content records) to a law enforcement agency.

Also, under the USA Patriot Act an Internet Service Provider may authorize federal law enforcement to investigate computer trespass by someone outside the system, e.g. a person that does not have an existing relationship with the owner or operator of the system.

A dialogue is going on between US and EU on arriving at a mutually acceptable "Safe Harbor" principle for personal data flowing from EU to USA. The proposal would allow U.S. companies to transfer data from the EU if they demonstrate compliance with "safe harbor principles."

Companies interested in qualifying for a safe harbor could do so in several ways, including by joining a private sector privacy program that adheres to the principles or by incorporating the principles into contracts with parties transferring information

from Europe. Because the principles largely reiterate the Directive's substantive standards, the proposal is unlikely to avoid the need for companies to address the Directive's basic requirements.

HIPAA (HEALTH, INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed in US Congress on August 21, 1996, as Public Law. It is a comprehensive legislation that addresses several issues of Health Care Management.

The primary purpose of the law is to provide continuity of healthcare coverage in situations such as employees changing organizations etc and prohibits discrimination against individuals based on health status. The Act also expands the weapons for combating fraud and abuse in health care delivery.The law also contains new requirements for the electronic transmission of health information. One of the essential features of the law is the protection of privacy of health data at every point of its storage and transmission and development of uniform standards for secure transmission of health information.

For example, the transmission of health related data has to be properly encrypted during transmission. Faxing of data or sending it as an unencrypted e-mail on a open network would amount to violation of the Act.. The implementation of the provisions have been staggered and full compliance of all the provisions is scheduled for April 2003.

The impact of HIPAA on Indian business houses dealing with

either data processing or software development will be in the form of HIPAA compliance standard becoming part of Quality management programmes in the Companies. Non Compliance of HIPAA could endanger the existing quality level certificates of these companies.

GLBA (GRAMM LEACH BLILEY ACT)

The Gramm Leach Bliley Act 1999 is another legislation in USA which focuses on the protection of financial information of individuals.

According to the Act, any financial institution that provides financial products or services to consumers must comply with the privacy provisions of the Act. These privacy regulations apply to all United States offices of financial institutions regardless of where the consumer lives.

The GLBA added new regulations in four main areas:

- disclosure of privacy policies;
- "opt-out" of information disclosures to non-affiliated third parties;
- non-disclosure of account information; and
- standards to protect security and confidentiality of consumers' non-public information.

As per the Act, the institutions should disclose their privacy policies to consumers annually. GLBA gives consumers the right to "opt-out" of allowing the institution to send non-public personal information to nonaffiliated third parties.

Even if the consumer does not opt-out, third parties may not re-

disclose this information.

Opt-out provision does not however apply to the sharing of information with third parties to process statements or service customer accounts.

Opt-out is also unnecessary when information is transferred to complete transactions authorized by the customer, when disclosing customer information to a credit bureau, complying with a regulatory investigation by state or federal authorities, or to protect against fraud.

Opt-outs are also not required for institutions that want to share information with affiliates — companies that are closely related through ownership by a parent company. This rule applies to all companies, not just financial institutions.

GLBA prohibits institutions from sharing account numbers or other similar identification numbers or codes with non-affiliated parties for the purposes of telemarketing, direct mail marketing, and marketing through e-mail solicitations.

Further, GLBA requires financial institution regulators to establish standards to ensure the confidentiality and security of consumer records, protect against threats to the security of those records, and protect against unauthorized access to those records that could result in substantial harm or inconvenience to the consumer.

The GLB Act's definition of "financial institution" includes banks, bank holding companies, securities firms, insurance companies, insurance agencies, thrifts, credit unions, mortgage brokers, finance companies, and check cashers. In addition,

because of the way GLB defines "financial activities," these protections will extend to travel agencies and may even apply to real estate brokers. Children Online Privacy Protection Act (COPPA)

The main objective of Children's Online Privacy Protection Act of 1998 (COPPA) is to protect the privacy of children using the Internet. With the publication of the rule, as of April 21, 2000, certain commercial Web sites must obtain parental consent before collecting, using, or disclosing personal information from children under 13.

Key Provisions of the Act

- **Privacy Notice on the Web Site**

  A Web site operator must post a clear and prominent link to a notice of its information practices on its home page and at each area where personal information is collected from children. The notice must state the name and contact information of all operators, the types of personal information collected from children, how such personal information is used, and whether personal information is disclosed to third parties.

  The notice also must state that the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary. In addition, the notice must state that the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information.

- **Verifiable Parental Consent**

The rules under the Act allows Web sites to vary their consent methods based on the intended uses of the child's information. For a two-year period, use of the more reliable methods of consent (print-and-send via postal mail or facsimile, use of a credit card or toll-free telephone number, digital signature, or e-mail accompanied by a PIN or password) will be required only for those activities that pose the greatest risks to the safety and privacy of children -- i.e., disclosing personal information to third parties or making it publicly available through chat rooms or other interactive activities.

For internal uses of information, such as an operator's marketing back to a child based on the child's personal information, operators will be permitted to use e-mail, as long as additional steps are taken to ensure that the parent is providing consent. Such steps could include sending a confirmatory e-mail to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call.

The "sliding scale" will sunset two years after the effective date of the rule, at which time the more reliable methods would be required for all uses of information, unless the Commission determines more secure electronic methods of consent are not widely available.

- **Choice Regarding Disclosures to Third Parties**

  The rules require operators to "give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties."

- **Online Activities for which Parental Consent is Not Required**

  The rule sets forth some exceptions to the requirement of prior parental consent that permit operators to collect a child's e-mail address for certain purposes. For example, no consent is required to respond to a one-time request by a child for "homework help" or other information. In addition, an operator can enter a child into a contest or send a child an online newsletter as long as the parent is given notice of these practices and an opportunity to prevent further use of the child's information.

- **Coverage of Information Submitted Online**

  The rule covers only information submitted online, and not information requested online but submitted offline.

- **Role of Schools in Obtaining Consent for Students**

  The schools can act as parents' agents or as intermediaries between Web sites and parents in the notice and consent process.

Dot-kids Domain space

One of the solutions that US is considering to protect Kids online is to pass a legislation to create a separate domain space for kids. A Bill called the Dot-Kids

Implementation and Efficiency Act, has already been passed by the US Senate which calls for the creation of a dot-kids domain within America's dot-us addressing space.

This is expected to provide the young generation a free Cyber space to browse through and benefit from the Internet revolution without the onslaught of pornography and other evils that confront the society. This would also make it easy for Schools and libraries to run child safe Internet browsing centers.

The bill also provides that Web site with a kids.us address cannot post hyperlinks to locations outside of the kids.us domain. It also prohibits chat and instant messaging features, except in cases where a site operator can guarantee the features adhere to kid-friendly standards developed for the domain.

If this strategy succeeds, it may be followed by other countries too.

In summary it is clear that Privacy protection of online data has been covered under multiple legislations in USA and are fairly stringent.

PRIVACY LAWS IN INDIA

ITA 2000 and Privacy Protection

The Information Technology Act-2000 has not addressed the issues of personal rights of Netizens. However, there is a mention

of consequences of the "Breach of Privacy and Confidentiality" under Section 72 of the Act.

According to the section,

> If any person who, in pursuance of any of the powers conferred under this Act has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned,
> - discloses such material to any other person,
> - he 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 .

Since this applies only to information secured in pursuance of a power conferred under this Act, it refers only to the Certifying Authorities, the Controller or his authorized investigating agencies who may come to possess personal data in the course of their work. This does not otherwise cover the personal rights of an individual.

We therefore need to look at legal aspects of privacy and freedom of speech from the law outside the ITA-2000. A brief discussion of the same is provided below.

INDIAN CONSTITUTION ON PRIVACY

The Supreme Court of India has stated in some of its judgments that Right to Privacy can be inferred from Article 21 in the Constitution though not enumerated as a Fundamental right.
India also guarantees freedom of speech through its constitution

to its citizens. These are the guiding principles even for the Netizens of India.

Extracts from the Constitution of India

FUNDAMENTAL RIGHTS

Article 21. Protection of life and personal liberty.-

No person shall be deprived of his life or personal liberty except according to procedure established by law.

…..

NEED FOR SPECIFIC DATA PROTECTION LAW IN INDIA

The need for a specific data protection law in India is heightened since the international laws apply to data exported to India for processing. Absence of data protection laws in India may even bar data processing business flowing into India.

It is therefore necessary for the country to either develop a suitable data protection law or the companies develop a suitable "Compliance Standard" that would meet the safe harbor principles that EU seems to be expecting from US and other countries.

NASSCOM has already mooted the idea of Data Protection Laws in India and action is expected in this regard in due course.

It must however be acknowledged that in a terrorist action prone country like India, the privacy laws cannot ignore the requirement of the law enforcement authorities to patrol and monitor objectionable activity. Hence ITA-2000 as well as POTA (Prevention of Terrorism Act) and the forthcoming Communication Convergence Act have provisions for interception of data by appropriate authorities under certain circumstances.

FREEDOM OF SPEECH

Having discussed the "Right to Privacy", it is also necessary for us to discuss the impact on the Cyber society of another fundamental human right in a democratic society namely "Freedom of Speech".

Freedom of speech, like the right to privacy is a restricted right in the sense that it is available only to the extent that it is not defamatory or fraudulent or a mis-representation of a fact.

The problem of Freedom of Speech Vs Defamation assumes greater importance on the Net because the Net makes any one a "publisher" by himself. On the Internet, there are many unmoderated News groups and E-mail lists where a person can post a defamatory message and publish it instantly. With a little additional effort, a person can create a website, which may aggregate and publish unsubstantiated defamatory information about some body without any hindrance.

Extracts from the Constitution of India

FUNDAMENTAL RIGHTS
Right to Freedom
19. Protection of certain rights regarding freedom of speech, etc.-

(1) All citizens shall have the right-

(a) to freedom of speech and expression; …..

…..(2) Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

……

Such defamation cases can be taken up by the offended person under the normal laws quoting the Website as a tool used for defamation.

Similar cases also arise in case of "Politically" sensitive information being placed on the web, which may even be a threat to the Integrity of a nation.

These are cases where the "Freedom" of speech is misused.

Most of the Governments would therefore like to control the web publishing activity through various means. In the simplest case it may be a simple monitoring through Carnivore kind of software so that when the freedom transcends the limit of tolerance, it can be treated as a crime and punished. At a more aggressive level, it may become "Censorship" with offending websites being taken off the net. It is to enable such control that many Governments are trying to take control of "Domain Name" Administration system away from ICANN.

The current trend suggests that the Cyber society may eventually come under the local physical governments for the purpose of determining the limits to "Freedom of Speech" on the Internet as applicable to persons who are citizens of such a country or live in or hold properties within the jurisdiction of such a country.

Activities which maybe considered as "Anti National" may be pursued as a Cyber Crime and violators could be rounded up even if they are in a different country through the operation of international treaties for Crime control.

In India, the "Right to Freedom of Speech" is not as aggressively defended by the community as in USA. At present the Indian society is watching two incidents of immense importance in this context. One is the action of the Police in Mumbai coming out with a guideline on "ID Cards for Cyber Cafe Users" and the other is a Public Interest Litigation in Delhi against the Government insisting on similar regulations by law. In both cases the regulation is meant to control the Internet usage through the intermediary Cyber Cafe. Perhaps the decision in the case of this PIL would mark a significant milestone in the establishment of the Freedom of Speech rights for Indian Netizens.

India as well as some other countries are also facing the problem of "Hate Sites" that preach cessation, communal hatred and other anti national propaganda. They are often promoted by citizens of countries like USA where the freedom of speech is well protected.

While the damage to internal peace and harmony of the country is by such sites is evident, the Indian Government has not been able to take adequate action on such sites.

In a recent incident in India the Government exhibited its inadequacy to apply its regulation for controlling adverse content on web. In a bid to block a yahoo group by name "kynhun" which is supposed to belong to an anti national Mizoram outfit, the Government issued an order to all ISPs to block the URL http//groups.yahoo.com/kynhun/. However most ISPs blocked the entire URL http://groups.yahoo.com shutting out lakhs of genuine yahoo groups containing discussions on many scientific, medical and other subjects beneficial to the community. The ISPs refused to accept that they can technically block only the group against which the order had been issued and instead imposed what may be called as an unfair censorship on a genuine activity.

This clearly demonstrated the difficulties that the regulator faces when the technical intermediaries do not cooperate.

In terms of procedures however the Government of India has prescribed through a notification that "Blocking of Websites" can be ordered by the "CERT- India" which functions from the Ministry of Information Technology based on a request from authorised officials. Such officials include IT Secretaries of the State Governments and Central Government besides CBI, NHRC and the Courts.

SPAM

An offshoot of the discussions on "Free Speech" and "Privacy" is "Spam" (unsolicited email). Spam also includes "Commercial Speech" which some say should be allowed within limits.

Recipients of Spam often consider it to be an unwanted intrusion in their mailbox. Internet Service Providers (ISPs), consider Spam to be a financial drain and an impediment to Internet access because it can clog an ISP's available bandwidth.

Not all bulk email is however Spam. Some bulk mails are permission based. This occurs when a user at a website voluntarily agrees - for example, at the time of making a purchase - to receive email or a newsletter (known as "opting-in"). Unlike Spam, opt-in email usually provides a benefit such as free information. Sending unsolicited email to online customers who have not elected to receive information is considered Spam.

In view of the strong sentiments against "Spam" as a violation of "E-mail Privacy", most reputed organizations avoid it. However there will be many irresponsible marketers who may continue to use Spam as a marketing tool unless forcibly prevented. Spam has been declared illegal in many parts of USA. Action is normally initiated on the ISP if its security system is lax enough to allow their servers to be used as "Spam servers". In India there is no special law on "Spam". However if a person is put to financial loss or mental agony as a result of unsolicited mails, he can initiate action for "harassment" against the offender if he can be identified.

Some of the ISP s in India have internally adopted some procedures which are meant to prevent SPAM. One of the means

adopted by them is to prevent "Bulk E-Mail" so that one cannot send a mail to more than say 10 members at a time.

The second method by which ISP s are trying to put a check on Spam and for which some legal backing is being sought is to disable what is referred to as "Relaying" in the SMTP server. SMTP server is the server which controls the out going mails at the ISP. When a client sends an e-mail, the SMTP server identifies the destination server to which the mail has to be forwarded by a reference IP address-Server name look up table and routes the message accordingly. "Relaying" is referred to when a person who is not authorized to use the SMTP server uses the same for sending bulk e-mails .

This method has some legal inconsistencies and raises issues of unfair business practice and forces change of digital identity of a user.

For example, let us say, a client raman@vsnl.com logs into internet using his ID ramansubbarao@eth.net and the ISP service of Dishnet.

The client cannot use his ID raman@vsnl.com in his outlook express for sending outward mails since the SMTP server at eth.net will reject it as a mail sent from a non customer since the e-mail ID is not @eth.net.

The VSNL server will also reject the mail because the user has not logged on using the VSNL account.

While it appears natural at first glance for a service provider to insist that his access account alone has to be used if SMTP services are to be made available, this gives raise to a peculiar

problem of "Changing the Digital Identity " of a person by force.

For example, the Digital identity raman@vsnl.com is a permanent name of the person on the Cyber space which could have been used for entering into Digital contracts. Hence any forced change of the same because raman@vsnl.com decides to stop using the access account of VSNL will lead to a situation similar to a person changing his name in the real world.

This situation can be rectified by the SMTP servers providing for authentication separate from authentication for Internet access.

Hopefully, when the ITA-2000 goes for a revision, some of these aspects of privacy and freedom of speech would be addressed.

CHAPTER XIII

LAW ENFORCEMENT ISSUES

After the enactment of ITA-2000, the role of Law Enforcement Agencies (LEA) in India has undergone a tremendous change. Some of the distinguishing features of the challenges posed by Cyber Crimes to the LEA s are briefly discussed here.

POWERS OF LAW ENFORCEMENT AGENCIES UNDER ITA-2000

ITA-2000 has recognized the complications involved in investigating Cyber crimes and has prescribed under Section 78 that

> "notwithstanding anything contained in the Code of Criminal Procedure, 1973, only a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act."

One of the most hotly discussed sections of the ITA-2000 has been the powers of the Police under Section 80.

According to this section,

> "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 authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act."

This section provides powers to search and arrest without warrants and obviously places some restrictions on the use of this extraordinary power.

Firstly, the power can be exercised only by police officers not below the rank of DSP s and only in a public place.

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.

It must be noted that the powers can be exercised based on a "Reasonable Suspicion" that a Crime has been committed or being committed or is about to be committed.

The Act also empowers any authorized officers of the Central and State Governments to exercise similar powers. But such authorization can be given only by the Central Government and not the State Government.

The section also mandates that where any person is arrested under this section by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

LIMITATIONS OF THE POWERS

The section 80 of the ITA-2000 is often interpreted both as "Excessive Powers" for the Police and "Restrictive Powers" for the Police by different sections of the society. Some have interpreted this section to mean that the Police have no powers to investigate , search and arrest in a "Private Place". But this is not the intention of the section. The section does not prevent the police from investigating, searching or arresting in a private place with an appropriate warrant.

Yet another point which is often discussed under this section is the coverage of the definition of "Public Place".

According to the section "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public. It is not clear if this definition is comprehensive enough to include Cyber Café's if they are using a "Members Only" policy.

As regards the power of confiscation of assets, section Sec 76 states that

> '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 there under has been or is being contravened, shall be liable to confiscation."

According to the amendments brought in for Section 65 B of the Indian Evidence Act, if in the act of a Crime, a series of computers have been involved, in any manner involving a successive operation, in whatever order, all the computers used for that purpose shall be treated as constituting a single computer.

In view of this, the powers of confiscation of electronic evidence extends beyond the Computer used by the perpetrator of the crime to any other computer in the network, physical or virtual.

IS IT A CRIME? OR AN ACCIDENT?

Cyber Crimes involve a high technology input. To understand whether an incident is a Crime or an Accident requires an understanding of technology. Many times crimes are committed through Trojans planted in innocent computers, spoofed IP or E-

mail addresses, stolen passwords or any other means of using computers of innocent people to commit crimes.

In the computer crime scenario, it is possible to simulate a situation such as A in Australia activating the revolver in the safe of B in Bangalore to kill C in California.

Many virus activities often send false alarms that renders an innocent person prima-facie guilty of a crime.

Some times what appears to be a crime may actually be a prank from a computer wiz kid with no malicious intentions.

In all such cases, Police need to understand the real nature of the incident and proceed cautiously not to harm innocent victims.

CONVICTION RATE NOT TO BE HIGH

Cyber Crimes also have a wide impact on the society since any crime can be committed with electronic documents. A murder can take place with manipulation of hospital data and frauds can be committed on a village farmer with false e-documents. Such cases need to be investigated and acted upon in every small police station in the country.

Hence it is not feasible always to ensure that an elite enforcement force will address Cyber Crime issues. Even untrained or semi trained police personnel in small towns therefore get involved in Cyber Crime management and sufficient allowances have to be made for wrong diagnosis, and avoidable mistakes.
The identification, collection, preservation, presentation and proving in a court of law of Cyber Evidence is an extremely difficult task and requires technical expertise at every point.

Much of the Cyber evidence is "Transient" in nature which makes it nearly impossible to be proved "Beyond Doubt".

It is therefore necessary to accept that the "Conviction rates" of cyber crimes will be much lower than in conventional cases. This is more a reflection of the challenges involved in proving Cyber evidence in the court as per our current system of accepted judicial procedures rather than the inefficiency of the LEA s.

THE JUDICIAL SYSTEM HAS TO ADAPT

Even though the Adjudicator and the Appellate Tribunals envisaged under the Act are capable of determining there own procedures for any enquiry or trial, unless there is a basic change of mind set amongst those who are going to be in charge of these institutions, radical departures from set norms may not materialize.

We will therefore see that a Cyber Case which happens by e-mails flying across continents as 0 's and 1's will have to be argued on the basis of print outs taken from various computers accompanied by volumes of certification which would take years for Courts to act upon.

Unless judges come out of the brick and mortar building and sit in secured chat rooms and conduct online proceedings, no Cyber crime case will ever be dealt with in a satisfactory time frame for the LEA s to do a reasonable job.

Further the use of alternate dispute resolution mechanisms where "Arbitrations" will be resorted to as a means of resolving

contractual disputes needs to be encouraged so that the judiciary can focus more on Cyber Crimes rather than resolving contractual disputes.

If such drastic changes in the system of trial are required to be brought about, it would be necessary for the Government to take the initiative. If not, it would be difficult for the conviction rates in Cyber Crimes reach even double digits.

THE POLICE IN INDIA ARE GETTING PREPARED

The Central Bureau of Investigations (CBI) has taken the lead in preparing the Indian Police force for meeting the needs of the Cyber Crime era with appropriate training of its personnel. Many State Governments have also followed suit. The National Crimes Record Bureau (NCRB) in the Ministry of Home affairs Delhi and the National Police Academy, Hyderabad are also conducting training programmes for senior IPS officers to sensitize them on Cyber Crimes.

The state of Tamil Nadu is in the forefront of Police education with a series of training programmes being conducted on Cyber Crimes at the Police Training College, in Chennai.

The state of Karnataka has launched the first "Cyber Police Station" in the country and has even envisaged registration of online FIR s.

The Mumbai Police were the first to set up a Cyber Crime Cell in any State in India and have enlisted the support of many experts from the private sector.

At the next stage, the LEAs needs to equip themselves with the tools of the trade for Cyber Patrolling, Cyber Intelligence, Cyber Investigation etc. to improve their effectiveness. Since most of the state Governments are strafed for funds, it would take some time for the Indian Police force to be adequately equipped. Until then, it would be necessary for the LEA s to work in close alliance with select private sector bodies to carry out their duties.

INTRA-INDIA COLLABORATION NETWORK

It is also necessary for the special cells set up in different states to tackle Cyber Crimes, to develop an organized information sharing network and a collaboration model so that we resolve the problem of Police jurisdiction smoothly.

Such a network can also use a set of "Registered Ethical Hackers" and "Private Individual Consultants" to help the local police not only at the times of search and seizure but also during routine patrolling and intelligence duties.

NEED FOR CYBER INSPECTORS AS A CADRE

In this context, it is worthwhile to note that the Electronic Communications and Transactions Act 2002 of the Republic of South Africa envisages appointment of "Cyber Inspectors" as an exclusive cadre from the employees of the Director General (Equivalent to Controller in India) with specific powers for investigation, intelligence gathering, search and seizure.

Even though the powers to appoint such persons is also available under ITA-2000, it is more in respect of adhoc investigations and not geared to creating a permanent cadre of Cyber Inspectors.

For Cyber Crime management to be succesful there is a need to enlist elite computer specialists who may be in permanent employment in private sector companies and Cyber Law specialists who may be in consultancy business of legal practice.

The Criminal Procedure Code already provides powers for the Police to call for private help if felt necessary on a case to case basis. However this is a less known fact of law enforcement and the public need to be educated in this regard to make them realize their obligations to the society. If therefore the Commissioner of Police issues a request (Notice?) to the network specialist of Satyam Infoway to assist the Police investigating team in the case of an alleged Cyber Crime, the Company has to spare the services of the specialist.

However, to avoid such requests being considered an unwanted burden, Indian Police have to embark on a programme of developing "A Voluntary Cyber Crime Task Force" in every city with the involvement of willing persons from the private sector.

This taskforce can also act as the coordinating center for certifying "Ethical Hackers" and "Friends of the Cyber Police". These persons can on merit be further recognized and drawn into the cadre of "Certified Cyber Inspectors" along with the Government employees appointed for the purpose.

NEED FOR INTERNATIONAL COOPERATION

Once an effective Intra-India cooperation of police forces is available, we can aim at similar cooperation treaties first between India and the South Asian countries and then extend it to Europe and American and Australian continents.

At present, there has not been much of an effort on the involvement of India in Cyber Crime Treaties being discussed around the world.

India has signed a cooperation treaty with Singapore in this regard which needs to be strengthened and activated. There have been bilateral discussions with USA following the September 11, 2001 terrorist attack in New York for the purpose of cooperating in the follow up investigations. Otherwise, the international cooperation has been mainly in the form of a request from the foreign investigating agency such as the FBI or the Scotland Yard to the CBI. CBI has in the past helped FBI in the investigation of "I Love You" virus and also in respect of a complaint of "Spam" from UK where a student in Pondicherry was tracked and arrested.

With a well developed software industry and being one of the early countries in the region to adopt Cyber Laws, India is well placed to lead a regional Cyber Crime Cooperation Treaty in South East Asia.

Such International Cooperation would be the key to improve the efficiency of LEA s in India to prevent incidence of Cyber Crimes.

CHAPTER XIV

E GOVERNANCE ISSUES

E-Governance is an important issue before the regulators today since it places the Governments in an uneasy situation of having to alter the status quo without knowing the full implications of the consequences.

E-Governance and ITA-2000

ITA-2000 has devoted a chapter for Electronic Governance and under sections 4 to 10 dealt with the different issues concerning the use of Information Technology for Electronic Governance.

While Section 4 and 5 provides the legal recognition for Electronic records and Electronic Signatures, sections 6, 7 and 8 provide the authority for any Government agency to use electronic documents for accepting any forms or tender application etc or receiving payments from the public or for retaining Government records or issue Gazette notifications.

Under Section 9 however, the Act has left it to the choice of these Government departments to adopt technology for any aspect of their administration and denied any right to the citizens to compel the Government bodies in this regard.

Sections 4 and 5 of the ITA-2000 which provide legal recognition for Electronic documents and Digital Signatures have already been discussed in greater detail in earlier chapters.

Let's therefore look now in some detail the other sections 6 to 9 of the ITA-2000 that directly relate to use of Electronic

documents in E-Governance.

Section 6 of ITA-2000 states:

(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 license, 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).

While Section (6) above covers the acceptability of Electronic documents in Government procedures Section (7) of ITA-2000 covers "Retention of Documents" in the Government in Electronic form.

It states:

(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, -

> (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 dispatch 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 dispatched 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. Publication of rules. regulation, etc.. in Electronic Gazette.

A Careful reading of this section suggests that this section has focused mainly on the retention of documents generated in the E-Governance process by virtue of the earlier section (6).

In cases where documents in the Government sector were originally generated in paper form and have been now digitized, if they are to be retained in Electronic form, it would be necessary according to this section to ensure that the format in which they are stored should be such as to enable demonstration of the fact that they accurately represent the documents as they were originally generated.

In view of this mandatory need, it becomes essential that any electronic document stored in E-Governance projects have to use some means of checking data integrity such as use of Digital Signatures.

During the first few years of E-Governance projects in India, the non availability of Digital Signatures in the marketplace had prompted Governments to ignore this fact. As a result, from the

date of passage of ITA-2000, documents generated and stored without Digital Signatures could cause a problem in establishing the legal validity of the documents.

Section 8 of ITA-2000 further extends the concept of E-Governance to the act of issuing of Gazette notifications in Electronic form.

Accordingly,

> 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, bye-law, notification or any other matters 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

Under the powers conferred on them by the ITA-2000, several Government agencies have already started adopting E-Governance strategies for Citizen interface.

THE PRESENT STATUS ON THE GROUND

To start with, almost all State Government and Central Government agencies today have web sites in which they share a volume of information with the public.

This "transparency" has helped the citizens to avoid the middlemen for such simple tasks such as finding out which form is to be submitted for a service.

Secondly, most Government functionaries today are available on e-mail and the citizens can reach to the highest executive or a minister in the country with his petition or complaint.

Even though not all politicians are prompt in attending to such e-complaints, there are many ministers and bureaucrats who are using this facility to improve the efficiencies of administration.

Thirdly, many Government departments have enabled utility payments such as electricity, telephone, water, Corporation tax etc to be made through the Internet avoiding the hassle of visiting different Government departments for routine matters.

E-GOVERNANCE INITIATIVE IN LAW MAKING

The Parliamentary Legislation department in particular, has been using Internet fairly effectively to elicit public opinion on various proposed laws at the formative stage. The Information Technology Bill itself was available on the net for more than two years before it became a law.

The Communication Convergence Bill has undergone major changes based on the reactions received from the public through the Internet.
These efforts of the law making bodies have not only enabled them to be transparent about their intentions and also use the valuable knowledge resources available in the public but also has stood as an example to many private sector companies to be more transparent in their business.

The Mumbai High Court went one step further in the case on Cyber Café regulation. In a celebrated suo-motu order in January

2002, the Mumbai high court ordered that an important report formulated by an expert committee set up earlier to suggest the Court on some of the regulatory aspects on Cyber Café's be placed on a web site to enable public to send their views.

It was an act of faith that the Court placed on the power of the Internet to collate views of the public before passing a judgment that could affect the society. This will stand in the history of development of E-Governance in India as an important milestone.

BENEFITS OF E-GOVERNANCE

As is evident in the above initiatives, the use of Internet has become a common tool for improving the efficiency of Citizen Governance in many ways.

More over, apart from promoting Transparency and Convenience, appropriate use of E-Governance will bring down the cost of administration substantially.

Further ,E-Governance properly harnessed could lead to new revenue generation prospects for the huge Government machinery which is under employed at present.

BUILDING CONFIDENCE WITH THE PUBLIC

However, if E-Governance has to succeed, people must have confidence in the system. If not, public will continue to use the paper based interface system defeating the purpose of E-Governance. Cyber Laws are the means through which the public will gain such confidence.

THE PROBLEM OF DIGITAL DIVIDE

One of the objectives of regulation is to ensure that in implementing E-Governance, the society does not get affected through a "Digital Divide" between the Digital Haves and Digital have-nots. Otherwise, the society will see the growth of anti social elements out of the affected sections of the society.

Section 9 of the ITA-2000 is aimed at ensuring this. This section leaves the decision to adopt E-Form of Governance to the Government departments and does not make it a matter of right to the Citizens.

It states:

> 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

At first glance , it appears that this section runs contrary to what the earlier three sections suggest. However, keeping in view the general need of the society to moderate the technological progress this is a cautious step that the Government has taken.

THE ROAD MAP OF E-GOVERNANCE INITIATIVES

The E-Governance initiatives of any Government starts with "Computerization" and "Connectivity" first. If the initiative has to be taken beyond this stage, it is necessary to ensure availability of appropriate "Content" and proper "Education" for the masses.

These will be the thrust areas in the coming days of E-Governance.

One of the hurdles for effective implementation of E-Governance projects is the lack of adequate funds with the State Governments. It is therefore necessary to reduce the cost of computerization through use of "Appropriate Hardware" and "Open Source software".

Additionally, E-Governance projects which could be revenue earning and self sustaining need to be identified for priority implementation.

E-GOVERNMENT

In discussing E-Governance, it is necessary for us to distinguish it with two other similar looking terms such as "E-Government" and "I-Governance".

E-Government is a term which is used to represent the use of Information Technology in the internal administration of the Government.
This involves computerization of internal processes, communication and information management system in order to improve the efficiency of the Government.

In contrast, E-Governance focuses on the use of technology in the Citizen interface.

I-GOVERNANCE

I-Governance on the other hand refers to the Governance of the Internet system itself.

Presently, the Internet system is governed through a control of the IP Addresses and Domain Names. IP address is the four quartet number such as 192.35.123.35 etc ,that is assigned to a computer connected to the Internet network. Without such an assignment of a number, a computer cannot connect to and be part of the Internet network.

By allowing or disallowing the use of an IP address a control can be exercised on the Netizens.

A second part of I-Governance is the control over the Domain Name System which is vital for web sites to be easily accessible to the public.

A third part of the I-Governance is the standardization of protocols used by various services that are part of the Internet system.

Since the birth of Internet as a project of the defense department of the Government of US most of the controls initially rested with the US Government . Later, as Internet became a public domain, the US Government gradually shifted the administration to autonomous bodies outside the Government's ambit. Out of several iterations today, an organization called ICANN (The Internet Corporation for Assigned Names and Numbers) has emerged as the apex administrative authority for Internet.

ICANN

Formed in October 1998, ICANN is a non-profit, private-sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities. ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.

COMPOSITION OF ICANN.

The Shanghai meeting of ICANN held between October 28 and October 31, 2002 adopted the following representative structure for ICANN management.

ICANN will be assisted in its functions by three supporting organizations: the GNSO (Generic Names Supporting Organization), the CNSO (Country Names Supporting Organization), and the ASO (Addressing Supporting Organization).

There will also be four standing advisory committees of the Board: the GAC (Government Advisory Committee), the TAC (Technical Advisory Committee), the RSSAC (the DNS Root Server System Advisory Committee) and the SAC (Security Advisory Committee).

The Board of ICANN will be comprised of 15 Directors. Additionally there shall be 6 non-voting Liaisons who may participate in Board discussions and deliberations like Directors but shall not cast votes. The 15 voting Directors shall be selected

as follows:

- 8 Directors selected by the Nominating Committee (NomCom)

- 2 Directors selected from each of the three Supporting Organizations
- The President of ICANN

The 6 non-voting Liaisons shall be selected as follows:

- 1 by the Technical Liaison Group
- 1 by the Internet Engineering Task Force
- 1 by the Root Server System Advisory Committee
- 1 by the Security and Stability Advisory Committee
- 1 by the Governmental Advisory Committee
- 1 by At Large Advisory Committee

The term of all the directors would be 3 years.

Together with its Board of Directors, ICANN builds consensus through the supporting organizations and the At Large representatives.

IPV4 and IPV 6 Systems

In the present system of four part IP addressing system (IPV4 System) where each part can take a value from 0 to 255, there are totally, 4 billion possible IP address combinations. Blocks of the addresses have been allocated to different countries and the ISP s who are operating therein.

Out of this block, certain numbers are assigned by ISP s for "Static IP addresses" to be given to those computers on the

network which needs to be accessed from others, such as the computers on which web sites are hosted.

Some IP addresses are kept for allotment to Internet users. Some of the users are allocated permanent IP addresses while others are allocated IP addresses whenever they connect to the internet from a pool of addresses kept for the purpose. These are called dynamic IP addresses and are normally allocated for dial up customers of an ISP.

It is estimated that within the next few years the growth on Internet usage particularly with the mobile phones becoming capable of internet connectivity, will exhaust the available IP addresses. In order to overcome this problem, the addressing system which is a four part system at present will be changed to a 6 part system. This addressing protocol referred to as IPV 6 protocol will make available a very large number of IP addresses for the use of the community.

Further the allocations in the IPV 4 system was historically skewed towards US which had 38 % of the addresses allocated. Countries in Asia mainly China and India had very low allocations. In the IPV 6 allocations, this anomaly needs to be corrected so that the needs of highly populated countries such as India are not overlooked.

Domain Name Allocation

Allocation of domain names is also governed by ICANN operating through a network of "Accredited Registrars" who allot the domain names to the Netizens upon application.

During such allotment, a name is allocated to an IP address through a domain name server of the ISP who hosts the web site.

ICANN has in consultation with WIPO (World Intellectual Property Organization) devised certain norms for dealing with the disputes arising out of allotment of domain names called the "Uniform Dispute Resolution Policy" which is the basis for controlling the domain name space.

All accredited registrars are made to adhere to the central norms fixed by ICANN and also make the domain name applicants agree to the norms through the contract signed at the time of domain name allocation.

PROTOCOL STANDARDIZATION

The third area of control which ICANN exercises is in the protocol standardization area. This is done through the Protocol Support organization (PSO). This organization now represents the various organizations that had emerged over a period for similar purposes such as the IETF (Internet Engineering Taskforce) and W3C Consortium (World wide Web Consortium) besides International Telecommunication Union and European Telecommunications Standards Institute.

The Protocol Supporting Organization (PSO) will be a consensus-based advisory body within the ICANN framework. The PSO will establish a "Protocol Council" and host an annual open meeting (the "General Assembly"). The Protocol Council will advise the ICANN Board on matters referred to the Protocol Council by the ICANN Board relating to the assignment of parameters for Internet protocols. It will also assist ICANN in all policy matters concerning the technical aspects of Internet.

Thus ICANN has substantial control over the Cyber space through the allocation of ID s for the computers which connect to the Internet and monitoring the technical standards that drive the Internet.

DEMOCRACY AT ICANN

For all practical purposes, therefore ICANN is the apex governing body of the Cyber space, much like the United Nations Organization.

However a universally acceptable Governing council of the ICANN is yet to emerge.

ICANN on its part tried to establish a democratic process of Governance through an out reach program Under its At Large Study Committee (ALSO) , it tried to enroll individual Netizens into a community to share information and allow participation in the policy making efforts. It even conducted a global election once to elect representatives to the board of ICANN from the At Large community.

However, ICANN has now given up the election approach for public participation in its Board due to the practical problems it encountered in the process. Now At Large Organizations will be represented at ICANN through the At Large Advisory Committee and a non voting observer in the Board.

CHALLENGE TO ICANN

In the recent days, some private enterprises such as New.net and Dotsworld.net have emerged the domain name control authority

of the ICANN. They have successfully introduced new domain name extensions outside the ICANN fold with the use of special software plug-in for the browsers.

At present, New.net claims that over 110 million Netizens have installed the necessary plug-in that can direct the browsers to the TLDs promoted by New.net such as .shop, .game, .kids, .travel, .ltd, etc.

This forms nearly 20 % of the Netizen population as of now and poses a significant threat to the authority of ICANN in the domain name space. ICANN will continue to however exercise its control on the number space and will remain the apex institution for all administrative matters concerning IP addresses.

INDIAN IP ADDRESS SPACE

Looking at the Indian IP address space, there is a lack of clear administrative structure.

NCST (National Center for Software Technology, Now known as CDAC, Center for Development of Advanced Computing), an autonomous society, involved in Research and Development, under the administrative purview of Department of Information Technology, Ministry of Communications and Information Technology, Government of India is the authority designated for registration of domain names with the Country Code ".in" (dot in).

NCST therefore exercises control over the allocation of domain names with the .in extension.
There are several ICANN accredited registrars who register other generic domain names who are directly controlled by ICANN.

The IP address space on the other hand is a more technical issue which concerns the business of ISP s. As long as VSNL was the monopoly ISP in India, it was the sole organization dealing with such matters. Now that VSNL has become a private enterprise and several other ISP s are also equally interested in the issue, a new authority has to take the responsibility for managing the IP address and domain name space relevant to India.

ITA-2000 has kept itself totally out of this issue. While the Communication Convergence Bill (discussed in detail in a subsequent chapter) has provided for setting up of a "Spectrum Manager" and "Spectrum Management Committee" to deal with the similar issue in the telecommunication sector, there has been no such authority designated for the purpose of negotiating with the international regime for IP address allocation.

It may be noted that South Africa has adopted an E-Commerce legislation which includes setting up of a domain name authority for the country.

At the time the Information Technology Bill was in the final stages of being passed, there was a brief discussion on bringing a "Domain Name Registration Authority" in India. However the proposal was not properly conceived and was presented as an additional domain name registering authority and did not elicit support.

NCST has adopted domain name registration polices which are highly user unfriendly and impractical and hence the total domain name registrations in the .in extension is hovering around 5465 in the first week of May 2003, after several years of its existence. This can be compared with more than 60,000 domain names being registered every day in the global market.

This represents a huge loss of potential and drainage of foreign exchange resources for the booking of other generic domain names by Indian residents.

Perhaps a well conceived Cyber Space Management Authority for India on the lines envisaged in South Africa should emerge to become the guiding force for Indian Internet community.

WORLD SUMMIT ON INFORMATION SOCIETY (WSIS)

In what can be termed as one of the most significant developments in the Governance of the Internet, a World Summit on Information Society (WSIS) had been organized under the United Nations leadership between December 10 to 12, 2003. More than 170 countries participated in the summit which discussed amongst other things whether the Governance of Internet has to be shifted from ICANN to an UN body such as the ITU.

The inaugural summit could not come to a conclusive agreement on the issue and decided to take up the issue in the next conference scheduled in Tunisia in 2005.

In the meantime the Geneva conference adopted a "Declaration of Principles" for the administration of the Information Society so as to reduce Digital Divide and also ensure that the Millennium Development Programme reaches the needy sections of the Global society. The draft declaration of Principles presented by Mr Kofi Annan, the Secretary UN is reproduced at the end of this chapter.

It also decided to set up a Working Group to develop an action plan which includes amongst other things how the Internet

Society Governance plan be funded.

A Copy of the action plan is reproduced at the end of the chapter.

India was represented by Mr Arun Shourie, the Minister of Communication and Information Technology who made a statement in the conference pledging India's contribution to the fund when developed in Cash and Kind.

This development could have significant impact on the future of the Internet since it could determine the regulatory aspects as well as the taxation aspects connected with the Internet.

Draft Declaration of Principles

Building the Information Society: a global challenge in the new Millennium

[Document WSIS-03/GENEVA/DOC/4-E dated 12 December 2003]

A. Our Common Vision of the Information Society

1. **We, the representatives of the peoples of the world**, **assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society,** declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.

2. **Our challenge** is to harness the potential of information and communication technology to promote the development goals of the Millennium Declaration, namely the eradication of extreme poverty and hunger; achievement of universal primary education; promotion of

gender equality and empowerment of women; reduction of child mortality; improvement of maternal health; to combat HIV/AIDS, malaria and other diseases; ensuring environmental sustainability; and development of global partnerships for development for the attainment of a more peaceful, just and prosperous world. We also reiterate our commitment to the achievement of sustainable development and agreed development goals, as contained in the Johannesburg Declaration and Plan of Implementation and the Monterrey Consensus, and other outcomes of relevant UN Summits.

3. **We reaffirm** the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration. We also reaffirm that democracy, sustainable development, and respect for human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing. We further resolve to strengthen respect for the rule of law in international as in national affairs.

4. **We reaffirm,** as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers.

5. **We further reaffirm** our commitment to the provisions of Article 29 of the Universal Declaration of Human Rights, that everyone has duties to the community in which alone the free and full development of their personality is possible, and that, in the exercise of their rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. These rights and freedoms may in no case be

exercised contrary to the purposes and principles of the United Nations. In this way, we shall promote an Information Society where human dignity is respected.

6. In keeping with the spirit of this declaration, **we rededicate ourselves** to upholding the principle of the sovereign equality of all States.

7. **We recognize that science** has a central role in the development of the Information Society. Many of the building blocks of the Information Society are the result of scientific and technical advances made possible by the sharing of research results.

8. **We recognize** that education, knowledge, information and communication are at the core of human progress, endeavour and well-being. Further, Information and Communication Technologies (ICTs) have an immense impact on virtually all aspects of our lives. The rapid progress of these technologies opens completely new opportunities to attain higher levels of development. The capacity of these technologies to reduce many traditional obstacles, especially those of time and distance, for the first time in history makes it possible to use the potential of these technologies for the benefit of millions of people in all corners of the world.

9. **We are aware** that ICTs should be regarded as tools and not as an end in themselves. Under favourable conditions, these technologies can be a powerful instrument, increasing productivity, generating economic growth, job creation and employability and improving the quality of life of all. They can also promote dialogue among people, nations and civilizations.

10. **We are also fully aware** that the benefits of the information technology revolution are today unevenly distributed between the developed and developing countries and within societies. We are fully committed to turning this digital divide into a digital opportunity for all, particularly for those who risk being left behind and being further marginalized.

11. **We are committed** to realising our common vision of the Information Society for ourselves and for future generations**.** We recognize that young people are the future workforce and leading creators and earliest adopters of ICTs. They must therefore be

empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet been able to benefit fully from the opportunities provided by ICTs. We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being.

12. **We affirm** that development of ICTs provides enormous opportunities for women, who should be an integral part of, and key actors, in the Information Society. We are committed to ensuring that the Information Society enables women's empowerment and their full participation on the basis on equality in all spheres of society and in all decision-making processes. To this end, we should mainstream a gender equality perspective and use ICTs as a tool to that end.

13. In building the Information Society, **we shall pay particular attention** to the special needs of marginalized and vulnerable groups of society, including migrants, internally displaced persons and refugees, unemployed and under-privileged people, minorities and nomadic people. We shall also recognize the special needs of older persons and persons with disabilities.

14. **We are resolute** to empower the poor, particularly those living in remote, rural and marginalized urban areas, to access information and to use ICTs as a tool to support their efforts to lift themselves out of poverty.

15. In the evolution of the Information Society, particular attention must be given to the special situation of indigenous peoples, as well as to the preservation of their heritage and their cultural legacy.

16. **We continue to pay** special attention to the particular needs of people of developing countries, countries with economies in transition, Least Developed Countries, Small Island Developing States, Landlocked Developing Countries, Highly Indebted Poor Countries, countries and territories under occupation, countries recovering from conflict and countries and regions with special needs as well as to conditions that pose severe threats to development, such as natural disasters.

17. **We recognize** that building an inclusive Information Society requires new forms of solidarity, partnership and cooperation among

governments and other stakeholders, i.e. the private sector, civil society and international organizations. Realizing that the ambitious goal of this Declaration—bridging the digital divide and ensuring harmonious, fair and equitable development for all—will require strong commitment by all stakeholders, we call for digital solidarity, both at national and international levels.

18. Nothing in this declaration shall be construed as impairing, contradicting, restricting or derogating from the provisions of the Charter of the United Nations and the Universal Declaration of Human Rights, any other international instrument or national laws adopted in furtherance of these instruments.

B. An information Society for all: key principles

19. **We are resolute** in our quest to ensure that everyone can benefit from the opportunities that ICTs can offer. We agree that to meet these challenges, all stakeholders should work together to: improve access to information and communication infrastructure and technologies as well as to information and knowledge; build capacity; increase confidence and security in the use of ICTs; create an enabling environment at all levels; develop and widen ICT applications; foster and respect cultural diversity; recognize the role of the media; address the ethical dimensions of the Information Society; and encourage international and regional cooperation. We agree that these are the key principles for building an inclusive Information Society.

1) The role of governments and all stakeholders in the promotion of ICTs for development

20. Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders.

2) Information and communication infrastructure: an essential foundation for an inclusive information society

21. Connectivity is a central enabling agent in building the Information Society. Universal, ubiquitous, equitable and affordable access to ICT

infrastructure and services, constitutes one of the challenges of the Information Society and should be an objective of all stakeholders involved in building it. Connectivity also involves access to energy and postal services, which should be assured in conformity with the domestic legislation of each country.

22. A well-developed information and communication network infrastructure and applications, adapted to regional, national and local conditions, easily-accessible and affordable, and making greater use of broadband and other innovative technologies where possible, can accelerate the social and economic progress of countries, and the well-being of all individuals, communities and peoples.

23. Policies that create a favourable climate for stability, predictability and fair competition at all levels should be developed and implemented in a manner that not only attracts more private investment for ICT infrastructure development but also enables universal service obligations to be met in areas where traditional market conditions fail to work. In disadvantaged areas, the establishment of ICT public access points in places such as post offices, schools, libraries and archives, can provide effective means for ensuring universal access to the infrastructure and services of the Information Society.

3) Access to information and knowledge

24. The ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society.

25. The sharing and strengthening of global knowledge for development can be enhanced by removing barriers to equitable access to information for economic, social, political, health, cultural, educational, and scientific activities and by facilitating access to public domain information, including by universal design and the use of assistive technologies.

26. A rich public domain is an essential element for the growth of the Information Society, creating multiple benefits such as an educated public, new jobs, innovation, business opportunities, and the advancement of sciences. Information in the public domain should be easily accessible to support the Information Society, and protected from

misappropriation. Public institutions such as libraries and archives, museums, cultural collections and other community-based access points should be strengthened so as to promote the preservation of documentary records and free and equitable access to information.

27. Access to information and knowledge can be promoted by increasing awareness among all stakeholders of the possibilities offered by different software models, including proprietary, open-source and free software, in order to increase competition, access by users, diversity of choice, and to enable all users to develop solutions which best meet their requirements. Affordable access to software should be considered as an important component of a truly inclusive Information Society.

28. We strive to promote universal access with equal opportunities for all to scientific knowledge and the creation and dissemination of scientific and technical information, including open access initiatives for scientific publishing.

4) Capacity building

29. Each person should have the opportunity to acquire the necessary skills and knowledge in order to understand, participate actively in, and benefit fully from, the Information Society and the knowledge economy. Literacy and universal primary education are key factors for building a fully inclusive information society, paying particular attention to the special needs of girls and women. Given the wide range of ICT and information specialists required at all levels, building institutional capacity deserves special attention.

30. The use of ICTs in all stages of education, training and human resource development should be promoted, taking into account the special needs of persons with disabilities and disadvantaged and vulnerable groups.

31. Continuous and adult education, re-training, life-long learning, distance-learning and other special services, such as telemedicine, can make an essential contribution to employability and help people benefit from the new opportunities offered by ICTs for traditional jobs, self-employment and new professions. Awareness and literacy in ICTs are an essential foundation in this regard.

32. Content creators, publishers, and producers, as well as teachers, trainers, archivists, librarians and learners, should play an active role in promoting the Information Society, particularly in the Least Developed Countries.

33. To achieve a sustainable development of the Information Society, national capability in ICT research and development should be enhanced. Furthermore, partnerships, in particular between and among developed and developing countries, including countries with economies in transition, in research and development, technology transfer, manufacturing and utilisation of ICT products and services are crucial for promoting capacity building and global participation in the Information Society. The manufacture of ICTs presents a significant opportunity for creation of wealth.

34. The attainment of our shared aspirations, in particular for developing countries, including countries with economies in transition, to become fully-fledged members of the Information Society, and their positive integration into the knowledge economy, depends largely on increased capacity building in the areas of education, technology know-how and access to information, which are major factors in determining development and competitiveness.

5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in co-operation with all stakeholders and international expert bodies. These efforts should be supported by increased international co-operation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

36. While recognizing the principles of universal and non-discriminatory access to ICTs for all nations, we support the activities of the United Nations to prevent the potential use of ICTs for purposes that

are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.

37. Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cyber-security should be dealt with at appropriate national and international levels.

6) Enabling environment

38. An enabling environment at national and international levels is essential for the Information Society. ICTs should be used as an important tool for good governance.

39. The rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centred Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, to maximize economic and social benefits, and to serve national priorities.

40. A dynamic and enabling international environment, supportive of foreign direct investment, transfer of technology, and international cooperation, particularly in the areas of finance, debt and trade, as well as full and effective participation of developing countries in global decision-making, are vital complements to national development efforts related to ICTs. Improving global affordable connectivity would contribute significantly to the effectiveness of these development efforts.

41. ICTs are an important enabler of growth through efficiency gains and increased productivity, in particular by small and medium sized enterprises (SMEs). In this regard, the development of the Information Society is important for broadly-based economic growth in both developed and developing economies. ICT-supported productivity gains and applied innovations across economic sectors should be fostered. Equitable distribution of the benefits contributes to poverty eradication and social development. Policies that foster productive investment and

enable firms, notably SMEs, to make the changes needed to seize the benefits from ICTs, are likely to be the most beneficial.

42. Intellectual Property protection is important to encourage innovation and creativity in the information society; similarly, the wide dissemination, diffusion, and sharing of knowledge is important to encourage innovation and creativity. Facilitating meaningful participation by all in intellectual property issues and knowledge sharing through full awareness and capacity building is a fundamental part of an inclusive Information Society.

43. Sustainable development can best be advanced in the Information Society when ICT-related efforts and programmes are fully integrated in national and regional development strategies. We welcome the New Partnership for Africa's Development (NEPAD) and encourage the international community to support the ICT-related measures of this initiative as well as those belonging to similar efforts in other regions. Distribution of the benefits of ICT-driven growth contributes to poverty eradication and sustainable development.

44. Standardization is one of the essential building blocks of the Information Society. There should be particular emphasis on the development and adoption of international standards. The development and use of open, interoperable, non-discriminatory and demand-driven standards that take into account needs of users and consumers is a basic element for the development and greater diffusion of ICTs and more affordable access to them, particularly in developing countries. International standards aim to create an environment where consumers can access services worldwide regardless of underlying technology.

45. The radio frequency spectrum should be managed in the public interest and in accordance with principle of legality, with full observance of national laws and regulation as well as relevant international agreements.

46. In building the Information Society, States are strongly urged to take steps with a view to the avoidance of, and refrain from, any unilateral measure not in accordance with international law and the Charter of the United Nations that impedes the full achievement of economic and social development by the population of the affected countries, and that hinders the well-being of their population.

47. Recognizing that ICTs are progressively changing our working practices, the creation of a secure, safe and healthy working environment, appropriate to the utilisation of ICTs, respecting all relevant international norms, is fundamental.

48. The Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.

49. The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

a) policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;

b) the private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;

c) civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;

d) intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;

e) international organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

50. International Internet governance issues should be addressed in a coordinated manner. We ask the Secretary-General of the United Nations to set up a working group on Internet governance, in an open and inclusive process that ensures a mechanism for the full and active

participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005.

7) ICT applications: benefits in all aspects of life

51. The usage and deployment of ICTs should seek to create benefits in all aspects of our daily life. ICT applications are potentially important in government operations and services, health care and health information, education and training, employment, job creation, business, agriculture, transport, protection of environment and management of natural resources, disaster prevention, and culture, and to promote eradication of poverty and other agreed development goals. ICTs should also contribute to sustainable production and consumption patterns and reduce traditional barriers, providing an opportunity for all to access local and global markets in a more equitable manner. Applications should be user-friendly, accessible to all, affordable, adapted to local needs in languages and cultures, and support sustainable development. To this effect, local authorities should play a major role in the provision of ICT services for the benefit of their populations.

8) Cultural diversity and identity, linguistic diversity and local content

52. Cultural diversity is the common heritage of humankind. The Information Society should be founded on and stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions, and foster dialogue among cultures and civilizations. The promotion, affirmation and preservation of diverse cultural identities and languages as reflected in relevant agreed United Nations documents including UNESCO's Universal Declaration on Cultural Diversity, will further enrich the Information Society.

53. The creation, dissemination and preservation of content in diverse languages and formats must be accorded high priority in building an inclusive Information Society, paying particular attention to the diversity of supply of creative work and due recognition of the rights

of authors and artists. It is essential to promote the production of and accessibility to all content—educational, scientific, cultural or recreational—in diverse languages and formats. The development of local content suited to domestic or regional needs will encourage social and economic development and will stimulate participation of all stakeholders, including people living in rural, remote and marginal areas.

54. The preservation of cultural heritage is a crucial component of identity and self–understanding of individuals that links a community to its past. The Information Society should harness and preserve cultural heritage for the future by all appropriate methods, including digitisation.

9) Media

55. We reaffirm our commitment to the principles of freedom of the press and freedom of information, as well as those of the independence, pluralism and diversity of media, which are essential to the Information Society. Freedom to seek, receive, impart and use information for the creation, accumulation and dissemination of knowledge are important to the Information Society. We call for the responsible use and treatment of information by the media in accordance with the highest ethical and professional standards. Traditional media in all their forms have an important role in the Information Society and ICTs should play a supportive role in this regard. Diversity of media ownership should be encouraged, in conformity with national law, and taking into account relevant international conventions. We reaffirm the necessity of reducing international imbalances affecting the media, particularly as regards infrastructure, technical resources and the development of human skills.

10) ETHICAL DIMENSIONS OF THE INFORMATION SOCIETY

56. The Information Society should respect peace and uphold the fundamental values of freedom, equality, solidarity, tolerance, shared responsibility, and respect for nature.

57. We acknowledge the importance of ethics for the Information Society, which should foster justice, and the dignity and worth of the human person. The widest possible protection should be accorded to the family and to enable it to play its crucial role in society.

58. The use of ICTs and content creation should respect human

rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments.

59. All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.

11) International and regional cooperation

60. We aim at making full use of the opportunities offered by ICTs in our efforts to reach the internationally agreed development goals, including those contained in the Millennium Declaration, and to uphold the key principles set forth in this Declaration. The Information Society is intrinsically global in nature and national efforts need to be supported by effective international and regional co-operation among governments, the private sector, civil society and other stakeholders, including the international financial institutions.

61.In order to build an inclusive global Information Society, we will seek and effectively implement concrete international approaches and mechanisms, including financial and technical assistance. Therefore, while appreciating ongoing ICT cooperation through various mechanisms, we invite all stakeholders to commit to the "Digital Solidarity Agenda" set forth in the Plan of Action. We are convinced that the worldwide agreed objective is to contribute to bridge the digital divide, promote access to ICTs, create digital opportunities, and benefit from the potential offered by ICTs for development. We recognize the will expressed on the one hand by some to create an international voluntary "Digital Solidarity Fund", and by others to undertake studies concerning existing mechanisms and the efficiency and feasibility of such a Fund.

62. Regional integration contributes to the development of the global Information Society and makes strong cooperation within and among regions indispensable. Regional dialogue should contribute to national capacity building and to the alignment of national strategies with the goals of this Declaration of Principles in a compatible way, while respecting national and regional particularities. In this context, we welcome and encourage the international community to support the

ICT-related measures of such initiatives.

63. We resolve to assist developing countries, LDCs and countries with economies in transition through the mobilization from all sources of financing, the provision of financial and technical assistance and by creating an environment conducive to technology transfer, consistent with the purposes of this Declaration and the Plan of Action.

64. The core competences of ITU in the fields of ICTs—assistance in bridging the digital divide, international and regional cooperation, radio spectrum management, standards development and the dissemination of information—are of crucial importance for building the Information Society.

C. Towards an Information Society for all based on shared knowledge

65. **We commit ourselves** to strengthening cooperation to seek common responses to the challenges and to the implementation of the Plan of Action, which will realize the vision of an inclusive Information Society based on the Key Principles incorporated in this Declaration.

66. **We further commit ourselves** to evaluate and follow-up progress in bridging the digital divide, taking into account different levels of development, so as to reach internationally agreed development goals, including those contained in the Millennium Declaration, and to assess the effectiveness of investment and international cooperation efforts in building the Information Society.

67. **We are firmly convinced** that we are collectively entering a new era of enormous potential, that of the Information Society and expanded human communication. In this emerging society, information and knowledge can be produced, exchanged, shared and communicated through all the networks of the world. All individuals can soon, if we take the necessary actions, together build a new Information Society based on shared knowledge and founded on global solidarity and a better mutual understanding between peoples and nations. We trust that these measures will open the way to the future development of a true knowledge society.

Plan of Action

[Document WSIS-03/GENEVA/DOC/5-E 12 December 2003]

A. INTRODUCTION

1. The common vision and guiding principles of the Declaration are translated in this Plan of Action into concrete action lines to advance the achievement of the internationally-agreed development goals, including those in the Millennium Declaration, the Monterrey Consensus and the Johannesburg Declaration and Plan of Implementation, by promoting the use of ICT-based products, networks, services and applications, and to help countries overcome the digital divide. The Information Society envisaged in the Declaration of Principles will be realized in cooperation and solidarity by governments and all other stakeholders.

2. The Information Society is an evolving concept that has reached different levels across the world, reflecting the different stages of development. Technological and other change is rapidly transforming the environment in which the Information Society is developed. The Plan of Action is thus an evolving platform to promote the Information Society at the national, regional and international levels. The unique two-phase structure of the World Summit on the Information Society (WSIS) provides an opportunity to take this evolution into account.

3. All stakeholders have an important role to play in the Information Society, especially through partnerships:

a) Governments have a leading role in developing and implementing comprehensive, forward looking and sustainable national e-strategies. The private sector and civil society, in dialogue with governments, have an important consultative role to play in devising national e-strategies.

b) The commitment of the private sector is important in developing and diffusing information and communication technologies (ICTs), for infrastructure, content and applications. The private sector is not only a market player but also plays a

role in a wider sustainable development context.

c) The commitment and involvement of civil society is equally important in creating an equitable Information Society, and in implementing ICT-related initiatives for development.

d) International and regional institutions, including international financial institutions, have a key role in integrating the use of ICTs in the development process and making available necessary resources for building the Information Society and for the evaluation of the progress made.

B. OBJECTIVES, GOALS AND TARGETS

4. The objectives of the Plan of Action are to build an inclusive Information Society; to put the potential of knowledge and ICTs at the service of development; to promote the use of information and knowledge for the achievement of internationally agreed development goals, including those contained in the Millennium Declaration; and to address new challenges of the Information Society, at the national, regional and international levels. Opportunity shall be taken in phase two of the WSIS to evaluate and assess progress made towards bridging the digital divide.

5. Specific targets for the Information Society will be established as appropriate, at the national level in the framework of national e-strategies and in accordance with national development policies, taking into account the different national circumstances. Such targets can serve as useful benchmarks for actions and for the evaluation of the progress made towards the attainment of the overall objectives of the Information Society.

6. Based on internationally agreed development goals, including those in the Millennium Declaration, which are premised on international cooperation, indicative targets may serve as global references for improving connectivity and access in the use of ICTs in promoting the objectives of the Plan of Action, to be achieved by 2015. These targets may be taken into account in the establishment of the national targets, considering the different national circumstances:

a) to connect villages with ICTs and establish community access points;

b) to connect universities, colleges, secondary schools and primary schools with ICTs;

c) to connect scientific and research centres with ICTs;

d) to connect public libraries, cultural centres, museums, post offices and archives with ICTs;

e) to connect health centres and hospitals with ICTs;

f) to connect all local and central government departments and establish websites and email addresses;

g) to adapt all primary and secondary school curricula to meet the challenges of the Information Society, taking into account national circumstances;

h) to ensure that all of the world's population have access to television and radio services;

i) to encourage the development of content and to put in place technical conditions in order to facilitate the presence and use of all world languages on the Internet;

j) to ensure that more than half the world's inhabitants have access to ICTs within their reach.

7. In giving effect to these objectives, goals and targets, special attention will be paid to the needs of developing countries, and in particular to countries, peoples and groups cited in paragraphs 11-16 of the Declaration of Principles.

C. ACTION LINES

C1. The role of governments and all stakeholders in the promotion of ICTs for development

8. The effective participation of governments and all stakeholders is vital in developing the Information Society requiring cooperation and partnerships among all of them.

a) Development of national e-strategies, including the necessary human capacity building, should be encouraged by all countries by 2005, taking into account different national circumstances.

b) Initiate at the national level a structured dialogue involving all relevant stakeholders, including through public/private partnerships, in devising e-strategies for the Information Society and for the exchange of best practices.

c) In developing and implementing national e-strategies, stakeholders should take into consideration local, regional and national needs and concerns. To maximize the benefits of initiatives undertaken, these should include the concept of sustainability. The private sector should be engaged in concrete projects to develop the Information Society at local, regional and national levels.

d) Each country is encouraged to establish at least one functioning Public/Private Partnership (PPP) or Multi-Sector Partnership (MSP), by 2005 as a showcase for future action.

e) Identify mechanisms, at the national, regional and international levels, for the initiation and promotion of partnerships among stakeholders of the Information Society.

f) Explore the viability of establishing multi-stakeholder portals for indigenous peoples at the national level.

g) By 2005, relevant international organizations and financial institutions should develop their own strategies for the use of ICTs for sustainable development, including sustainable production and consumption patterns and as an effective instrument to help achieve the goals expressed in the United Nations Millennium Declaration.

h) International organizations should publish, in their areas of competence, including on their website, reliable information submitted by relevant stakeholders on successful experiences of mainstreaming ICTs.

i) Encourage a series of related measures, including, among other things: incubator schemes, venture capital investments (national and international), government investment funds (including micro-finance for Small, Medium-sized and Micro Enterprises (SMMEs), investment promotion strategies, software export support activities (trade counseling), support of research and development networks and software parks.

C2. Information and communication infrastructure: an essential foundation for the Information Society

9. Infrastructure is central in achieving the goal of digital inclusion, enabling universal, sustainable, ubiquitous and affordable access to ICTs by all, taking into account relevant solutions already in place in developing countries and countries with economies in transition, to provide sustainable connectivity and access to remote and marginalized areas at national and regional levels.

a) Governments should take action, in the framework of national development policies, in order to support an enabling and competitive

environment for the necessary investment in ICT infrastructure and for the development of new services.

b) In the context of national e-strategies, devise appropriate universal access policies and strategies, and their means of implementation, in line with the indicative targets, and develop ICT connectivity indicators.

c) In the context of national e-strategies, provide and improve ICT connectivity for all schools, universities, health institutions, libraries, post offices, community centres, museums and other institutions accessible to the public, in line with the indicative targets.

d) Develop and strengthen national, regional and international broadband network infrastructure, including delivery by satellite and other systems, to help in providing the capacity to match the needs of countries and their citizens and for the delivery of new ICT-based services. Support technical, regulatory and operational studies by the International Telecommunication Union (ITU) and, as appropriate, other relevant international organizations in order to:

i) broaden access to orbital resources, global frequency harmonization and global systems standardization;

ii) encourage public/private partnership;

iii) promote the provision of global high-speed satellite services for underserved areas such as remote and sparsely populated areas;

iv) explore other systems that can provide high-speed connectivity.

e) In the context of national e-strategies, address the special requirements of older people, persons with disabilities, children, especially marginalized children and other disadvantaged and vulnerable groups, including by appropriate educational administrative and legislative measures to ensure their full inclusion in the Information Society.

f) Encourage the design and production of ICT equipment and services so that everyone, has easy and affordable access to them including older people, persons with disabilities, children, especially marginalized children, and other disadvantaged and vulnerable groups, and promote the development of technologies, applications, and content suited to their needs, guided by the Universal Design Principle and further enhanced by the use of assistive technologies.

g) In order to alleviate the challenges of illiteracy, develop affordable technologies and non-text based computer interfaces to facilitate people's access to ICT,

h) Undertake international research and development efforts aimed at

making available adequate and affordable ICT equipment for end users.

i) Encourage the use of unused wireless capacity, including satellite, in developed countries and in particular in developing countries, to provide access in remote areas, especially in developing countries and countries with economies in transition, and to improve low-cost connectivity in developing countries. Special concern should be given to the Least Developed Countries in their efforts in establishing telecommunication infrastructure.

j) Optimize connectivity among major information networks by encouraging the creation and development of regional ICT backbones and Internet exchange points, to reduce interconnection costs and broaden network access.

k) Develop strategies for increasing affordable global connectivity, thereby facilitating improved access. Commercially negotiated Internet transit and interconnection costs should be oriented towards objective, transparent and non-discriminatory parameters, taking into account ongoing work on this subject.

l) Encourage and promote joint use of traditional media and new technologies.

C3. Access to information and knowledge

10. ICTs allow people, anywhere in the world, to access information and knowledge almost instantaneously. Individuals, organizations and communities should benefit from access to knowledge and information.

a) Develop policy guidelines for the development and promotion of public domain information as an important international instrument promoting public access to information.

b) Governments are encouraged to provide adequate access through various communication resources, notably the Internet, to public official information. Establishing legislation on access to information and the preservation of public data, notably in the area of the new technologies, is encouraged.

c) Promote research and development to facilitate accessibility of ICTs for all, including disadvantaged, marginalized and vulnerable groups.

d) Governments, and other stakeholders, should establish sustainable multi-purpose community public access points, providing affordable or free-of-charge access for their citizens to the various communication resources, notably the Internet. These access points should, to the extent

possible, have sufficient capacity to provide assistance to users, in libraries, educational institutions, public administrations, post offices or other public places, with special emphasis on rural and underserved areas, while respecting intellectual property rights (IPRs) and encouraging the use of information and sharing of knowledge.

e) Encourage research and promote awareness among all stakeholders of the possibilities offered by different software models, and the means of their creation, including proprietary, open-source and free software, in order to increase competition, freedom of choice and affordability, and to enable all stakeholders to evaluate which solution best meets their requirements.

f) Governments should actively promote the use of ICTs as a fundamental working tool by their citizens and local authorities. In this respect, the international community and other stakeholders should support capacity building for local authorities in the widespread use of ICTs as a means of improving local governance.

g) Encourage research on the Information Society, including on innovative forms of networking, adaptation of ICT infrastructure, tools and applications that facilitate accessibility of ICTs for all, and disadvantaged groups in particular.

h) Support the creation and development of a digital public library and archive services, adapted to the Information Society, including reviewing national library strategies and legislation, developing a global understanding of the need for "hybrid libraries", and fostering worldwide cooperation between libraries.

i) Encourage initiatives to facilitate access, including free and affordable access to open access journals and books, and open archives for scientific information.

j) Support research and development of the design of useful instruments for all stakeholders to foster increased awareness, assessment, and evaluation of different software models and licences, so as to ensure an optimal choice of appropriate software that will best contribute to achieving development goals within local conditions.

C4. Capacity building

11. Everyone should have the necessary skills to benefit fully from the Information Society. Therefore capacity building and ICT literacy are essential. ICTs can contribute to achieving universal education worldwide, through delivery of education and training of teachers, and offering improved conditions for lifelong learning, encompassing people that are outside the formal education

process, and improving professional skills.

a) Develop domestic policies to ensure that ICTs are fully integrated in education and training at all levels, including in curriculum development, teacher training, institutional administration and management, and in support of the concept of lifelong learning.

b) Develop and promote programmes to eradicate illiteracy using ICTs at national, regional and international levels.

c) Promote e-literacy skills for all, for example by designing and offering courses for public administration, taking advantage of existing facilities such as libraries, multipurpose community centres, public access points and by establishing local ICT training centres with the cooperation of all stakeholders. Special attention should be paid to disadvantaged and vulnerable groups.

d) In the context of national educational policies, and taking into account the need to eradicate adult illiteracy, ensure that young people are equipped with knowledge and skills to use ICTs, including the capacity to analyse and treat information in creative and innovative ways, share their expertise and participate fully in the Information Society.

e) Governments, in cooperation with other stakeholders, should create programmes for capacity building with an emphasis on creating a critical mass of qualified and skilled ICT professionals and experts.

f) Develop pilot projects to demonstrate the impact of ICT-based alternative educational delivery systems, notably for achieving Education for All targets, including basic literacy targets.

g) Work on removing the gender barriers to ICT education and training and promoting equal training opportunities in ICT-related fields for women and girls. Early intervention programmes in science and technology should target young girls with the aim of increasing the number of women in ICT careers. Promote the exchange of best practices on the integration of gender perspectives in ICT education.

h) Empower local communities, especially those in rural and underserved areas, in ICT use and promote the production of useful and socially meaningful content for the benefit of all.

i) Launch education and training programmes, where possible using information networks of traditional nomadic and indigenous peoples, which provide opportunities to fully participate in the Information Society.

j) Design and implement regional and international cooperation activities

to enhance the capacity, notably, of leaders and operational staff in developing countries and LDCs, to apply ICTs effectively in the whole range of educational activities. This should include delivery of education outside the educational structure, such as the workplace and at home.

k) Design specific training programmes in the use of ICTs in order to meet the educational needs of information professionals, such as archivists, librarians, museum professionals, scientists, teachers, journalists, postal workers and other relevant professional groups. Training of information professionals should focus not only on new methods and techniques for the development and provision of information and communication services, but also on relevant management skills to ensure the best use of technologies. Training of teachers should focus on the technical aspects of ICTs, on development of content, and on the potential possibilities and challenges of ICTs.

l) Develop distance learning, training and other forms of education and training as part of capacity building programmes. Give special attention to developing countries and especially LDCs in different levels of human resources development.

m) Promote international and regional cooperation in the field of capacity building, including country programmes developed by the United Nations and its Specialized Agencies

n) Launch pilot projects to design new forms of ICT-based networking, linking education, training and research institutions between and among developed and developing countries and countries with economies in transition.

o) Volunteering, if conducted in harmony with national policies and local cultures, can be a valuable asset for raising human capacity to make productive use of ICT tools and build a more inclusive Information Society. Activate volunteer programmes to provide capacity building on ICT for development, particularly in developing countries.

p) Design programmes to train users to develop self-learning and self-development capacities.

C5. Building confidence and security in the use of ICTs

12. Confidence and security are among the main pillars of the Information Society.

a) Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user

confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.

b) Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.

d) Take appropriate action on spam at national and international levels.

e) Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.

f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.

g) Share good practices in the field of information security and network security and encourage their use by all parties concerned.

h) Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response.

i) Encourage further development of secure and reliable applications to facilitate online transactions.

j) Encourage interested countries to contribute actively to the ongoing United Nations activities to build confidence and security in the use of ICTs.

C6. Enabling environment

13. To maximize the social, economic and environmental benefits of the Information Society, governments need to create a trustworthy, transparent and

non-discriminatory legal, regulatory and policy environment. Actions include:

a) Governments should foster a supportive, transparent, pro-competitive and predictable policy, legal and regulatory framework, which provides the appropriate incentives to investment and community development in the Information Society.

b) We ask the Secretary General of the United Nations to set up a working group on Internet governance, in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005. The group should, *inter alia*:

i) develop a working definition of Internet governance;

ii) identify the public policy issues that are relevant to Internet governance;

iii) develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organisations and other forums as well as the private sector and civil society from both developing and developed countries;

iv) prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005.

c) Governments are invited to:

i) facilitate the establishment of national and regional Internet Exchange Centres;

ii) manage or supervise, as appropriate, their respective country code top-level domain name (ccTLD);

iii) promote awareness of the Internet.

d) In cooperation with the relevant stakeholders, promote regional root servers and the use of internationalized domain names in order to overcome barriers to access.

e) Governments should continue to update their domestic consumer protection laws to respond to the new requirements of the Information Society.

f) Promote effective participation by developing countries and countries with economies in transition in international ICT forums and create

opportunities for exchange of experience.

g) Governments need to formulate national strategies, which include e-government strategies, to make public administration more transparent, efficient and democratic.

h) Develop a framework for the secure storage and archival of documents and other electronic records of information.

i) Governments and stakeholders should actively promote user education and awareness about online privacy and the means of protecting privacy.

j) Invite stakeholders to ensure that practices designed to facilitate electronic commerce also permit consumers to have a choice as to whether or not to use electronic communication.

k) Encourage the ongoing work in the area of effective dispute settlement systems, notably alternative dispute resolution (ADR), which can promote settlement of disputes.

l) Governments, in collaboration with stakeholders, are encouraged to formulate conducive ICT policies that foster entrepreneurship, innovation and investment, and with particular reference to the promotion of participation by women.

m) Recognising the economic potential of ICTs for Small and Medium-Sized Enterprises (SMEs), they should be assisted in increasing their competitiveness by streamlining administrative procedures, facilitating their access to capital and enhancing their capacity to participate in ICT-related projects.

n) Governments should act as model users and early adopters of e-commerce in accordance with their level of socio-economic development.

o) Governments, in cooperation with other stakeholders, should raise awareness of the importance of international interoperability standards for global e-commerce.

p) Governments, in cooperation with other stakeholders, should promote the development and use of open, interoperable, non-discriminatory and demand-driven standards.

q) ITU, pursuant to its treaty capacity, coordinates and allocates frequencies with the goal of facilitating ubiquitous and affordable access.

r) Additional steps should be taken in ITU and other regional organisations to ensure rational, efficient and economical use of, and equitable access to, the radio-frequency spectrum by all countries, based on relevant international agreements.

C7. ICT applications: benefits in all aspects of life

14. ICT applications can support sustainable development, in the fields of public administration, business, education and training, health, employment, environment, agriculture and science within the framework of national e-strategies. This would include actions within the following sectors:

15. E-government

a) Implement e-government strategies focusing on applications aimed at innovating and promoting transparency in public administrations and democratic processes, improving efficiency and strengthening relations with citizens.

b) Develop national e-government initiatives and services, at all levels, adapted to the needs of citizens and business, to achieve a more efficient allocation of resources and public goods.

c) Support international cooperation initiatives in the field of e-government, in order to enhance transparency, accountability and efficiency at all levels of government.

16. E-business

a) Governments, international organizations and the private sector, are encouraged to promote the benefits of international trade and the use of e-business, and promote the use of e-business models in developing countries and countries with economies in transition.

b) Through the adoption of an enabling environment, and based on widely available Internet access, governments should seek to stimulate private sector investment, foster new applications, content development and public/private partnerships.

c) Government policies should favour assistance to, and growth of SMMEs, in the ICT industry, as well as their entry into e-business, to stimulate economic growth and job creation as an element of a strategy for poverty reduction through wealth creation.

17. E-learning (see section C4)

18. E-health

a) Promote collaborative efforts of governments, planners, health professionals, and other agencies along with the participation of international organizations for creating a reliable, timely, high quality and affordable health care and health information systems and for promoting continuous medical training, education, and research through the use of

ICTs, while respecting and protecting citizens' right to privacy.

b) Facilitate access to the world's medical knowledge and locally-relevant content resources for strengthening public health research and prevention programmes and promoting women's and men's health, such as content on sexual and reproductive health and sexually transmitted infections, and for diseases that attract full attention of the world including HIV/AIDS, malaria and tuberculosis.

c) Alert, monitor and control the spread of communicable diseases, through the improvement of common information systems.

d) Promote the development of international standards for the exchange of health data, taking due account of privacy concerns.

e) Encourage the adoption of ICTs to improve and extend health care and health information systems to remote and underserved areas and vulnerable populations, recognising women's roles as health providers in their families and communities.

f) Strengthen and expand ICT-based initiatives for providing medical and humanitarian assistance in disasters and emergencies.

19. E-employment

a) Encourage the development of best practices for e-workers and e-employers built, at the national level, on principles of fairness and gender equality, respecting all relevant international norms.

b) Promote new ways of organizing work and business with the aim of raising productivity, growth and well-being through investment in ICTs and human resources.

c) Promote teleworking to allow citizens, particularly in the developing countries, LDCs, and small economies, to live in their societies and work anywhere, and to increase employment opportunities for women, and for those with disabilities. In promoting teleworking, special attention should be given to strategies promoting job creation and the retention of the skilled working force.

d) Promote early intervention programmes in science and technology that should target young girls to increase the number of women in ICT carriers.

20. E-environment

a) Governments, in cooperation with other stakeholders are encouraged to use and promote ICTs as an instrument for environmental protection and the sustainable use of natural resources.

b) Government, civil society and the private sector are encouraged to initiate actions and implement projects and programmes for sustainable production and consumption and the environmentally safe disposal and recycling of discarded hardware and components used in ICTs.

c) Establish monitoring systems, using ICTs, to forecast and monitor the impact of natural and man-made disasters, particularly in developing countries, LDCs and small economies.

21. E-agriculture

a) Ensure the systematic dissemination of information using ICTs on agriculture, animal husbandry, fisheries, forestry and food, in order to provide ready access to comprehensive, up-to-date and detailed knowledge and information, particularly in rural areas.

b) Public-private partnerships should seek to maximize the use of ICTs as an instrument to improve production (quantity and quality).

22. E-science

a) Promote affordable and reliable high-speed Internet connection for all universities and research institutions to support their critical role in information and knowledge production, education and training, and to support the establishment of partnerships, cooperation and networking between these institutions.

b) Promote electronic publishing, differential pricing and open access initiatives to make scientific information affordable and accessible in all countries on an equitable basis.

c) Promote the use of peer-to-peer technology to share scientific knowledge and pre-prints and reprints written by scientific authors who have waived their right to payment.

d) Promote the long-term systematic and efficient collection, dissemination and preservation of essential scientific digital data, for example, population and meteorological data in all countries.

e) Promote principles and metadata standards to facilitate cooperation and effective use of collected scientific information and data as appropriate to conduct scientific research.

C8. Cultural diversity and identity, linguistic diversity and local content

23. Cultural and linguistic diversity, while stimulating respect for cultural identity, traditions and religions, is essential to the development of an Information Society

based on the dialogue among cultures and regional and international cooperation. It is an important factor for sustainable development.

a) Create policies that support the respect, preservation, promotion and enhancement of cultural and linguistic diversity and cultural heritage within the Information Society, as reflected in relevant agreed United Nations documents, including UNESCO's Universal Declaration on Cultural Diversity. This includes encouraging governments to design cultural policies to promote the production of cultural, educational and scientific content and the development of local cultural industries suited to the linguistic and cultural context of the users.

b) Develop national policies and laws to ensure that libraries, archives, museums and other cultural institutions can play their full role of content—including traditional knowledge—providers in the Information Society, more particularly by providing continued access to recorded information.

c) Support efforts to develop and use ICTs for the preservation of natural and, cultural heritage, keeping it accessible as a living part of today's culture. This includes developing systems for ensuring continued access to archived digital information and multimedia content in digital repositories, and support archives, cultural collections and libraries as the memory of humankind.

d) Develop and implement policies that preserve, affirm, respect and promote diversity of cultural expression and indigenous knowledge and traditions through the creation of varied information content and the use of different methods, including the digitization of the educational, scientific and cultural heritage.

e) Support local content development, translation and adaptation, digital archives, and diverse forms of digital and traditional media by local authorities. These activities can also strengthen local and indigenous communities.

f) Provide content that is relevant to the cultures and languages of individuals in the Information Society, through access to traditional and digital media services.

g) Through public/private partnerships, foster the creation of varied local and national content, including that available in the language of users, and give recognition and support to ICT-based work in all artistic fields.

h) Strengthen programmes focused on gender-sensitive curricula in formal and non-formal education for all and enhancing communication

and media literacy for women with a view to building the capacity of girls and women to understand and to develop ICT content.

i) Nurture the local capacity for the creation and distribution of software in local languages, as well as content that is relevant to different segments of population, including non-literate, persons with disabilities, disadvantaged and vulnerable groups especially in developing countries and countries with economies in transition.

j) Give support to media based in local communities and support projects combining the use of traditional media and new technologies for their role in facilitating the use of local languages, for documenting and preserving local heritage, including landscape and biological diversity, and as a means to reach rural and isolated and nomadic communities.

k) Enhance the capacity of indigenous peoples to develop content in their own languages.

l) Cooperate with indigenous peoples and traditional communities to enable them to more effectively use and benefit from the use of their traditional knowledge in the Information Society.

m) Exchange knowledge, experiences and best practices on policies and tools designed to promote cultural and linguistic diversity at regional and sub-regional levels. This can be achieved by establishing regional, and sub-regional working groups on specific issues of this Plan of Action to foster integration efforts.

n) Assess at the regional level the contribution of ICT to cultural exchange and interaction, and based on the outcome of this assessment, design relevant programmes.

o) Governments, through public/private partnerships, should promote technologies and R&D programmes in such areas as translation, iconographies, voice-assisted services and the development of necessary hardware and a variety of software models, including proprietary, open source software and free software, such as standard character sets, language codes, electronic dictionaries, terminology and thesauri, multilingual search engines, machine translation tools, internationalized domain names, content referencing as well as general and application software.

C9. Media

24. The media—in their various forms and with a diversity of ownership—as an actor, have an essential role in the development of the Information Society and

are recognized as an important contributor to freedom of expression and plurality of information.

a) Encourage the media—print and broadcast as well as new media—to continue to play an important role in the Information Society.

b) Encourage the development of domestic legislation that guarantees the independence and plurality of the media.

c) Take appropriate measures—consistent with freedom of expression—to combat illegal and harmful content in media content.

d) Encourage media professionals in developed countries to establish partnerships and networks with the media in developing ones, especially in the field of training.

e) Promote balanced and diverse portrayals of women and men by the media.

f) Reduce international imbalances affecting the media, particularly as regards infrastructure, technical resources and the development of human skills, taking full advantage of ICT tools in this regard.

g) Encourage traditional media to bridge the knowledge divide and to facilitate the flow of cultural content, particularly in rural areas.

C10. Ethical dimensions of the Information Society

25. The Information Society should be subject to universally held values and promote the common good and to prevent abusive uses of ICTs.

a) Take steps to promote respect for peace and to uphold the fundamental values of freedom, equality, solidarity, tolerance, shared responsibility, and respect for nature.

b) All stakeholders should increase their awareness of the ethical dimension of their use of ICTs.

c) All actors in the Information Society should promote the common good, protect privacy and personal data and take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.

d) Invite relevant stakeholders, especially the academia, to continue research on ethical dimensions of ICTs.

C11. International and regional cooperation

26. International cooperation among all stakeholders is vital in implementation of this plan of action and needs to be strengthened with a view to promoting universal access and bridging the digital divide, *inter alia*, by provision of means of implementation.

a) Governments of developing countries should raise the relative priority of ICT projects in requests for international cooperation and assistance on infrastructure development projects from developed countries and international financial organizations.

b) Within the context of the UN's Global Compact and building upon the United Nations Millennium Declaration, build on and accelerate public-private partnerships, focusing on the use of ICT in development.

c) Invite international and regional organizations to mainstream ICTs in their work programmes and to assist all levels of developing countries, to be involved in the preparation and implementation of national action plans to support the fulfilment of the goals indicated in the declaration of principles and in this Plan of Action, taking into account the importance of regional initiatives.

D. Digital Solidarity Agenda

27. The Digital Solidarity Agenda aims at putting in place the conditions for mobilizing human, financial and technological resources for inclusion of all men and women in the emerging Information Society. Close national, regional and international cooperation among all stakeholders in the implementation of this Agenda is vital. To overcome the digital divide, we need to use more efficiently existing approaches and mechanisms and fully explore new ones, in order to provide financing for the development of infrastructure, equipment, capacity building and content, which are essential for participation in the Information Society.

D1. Priorities and strategies

a) National e-strategies should be made an integral part of national development plans, including Poverty Reduction Strategies.

b) ICTs should be fully mainstreamed into strategies for Official Development Assistance (ODA) through more effective donor information-sharing and co-ordination, and through analysis and sharing of best practices and lessons learned from experience with ICT-for-development programmes.

D2. Mobilizing resources

a) All countries and international organizations should act to create conditions conducive to increasing the availability and effective mobilization of resources for financing development as elaborated in the Monterrey Consensus.

b) Developed countries should make concrete efforts to fulfil their international commitments to financing development including the Monterrey Consensus, in which developed countries that have not done so are urged to make concrete efforts towards the target of 0.7 per cent of gross national product (GNP) as ODA to developing countries and 0.15 to 0.20 per cent of GNP of developed countries to least developed countries.

c) For those developing countries facing unsustainable debt burdens, we welcome initiatives that have been undertaken to reduce outstanding indebtedness and invite further national and international measures in that regard, including, as appropriate, debt cancellation and other arrangements. Particular attention should be given to enhancing the Heavily Indebted Poor Countries initiative. These initiatives would release more resources that may be used for financing ICT for development projects.

d) Recognizing the potential of ICT for development we furthermore advocate:

i) developing countries to increase their efforts to attract major private national and foreign investments for ICTs through the creation of a transparent, stable and predictable enabling investment environment;

ii) developed countries and international financial organisations to be responsive to the strategies and priorities of ICTs for development, mainstream ICTs in their work programmes, and assist developing countries and countries with economies in transition to prepare and implement their national e-strategies. Based on the priorities of national development plans and implementation of the above commitments, developed countries should increase their efforts to provide more financial resources to developing countries in harnessing ICTs for development;

iii) the private sector to contribute to the implementation of this Digital Solidarity Agenda.

e) In our efforts to bridge the digital divide, we should promote, within our development cooperation, technical and financial assistance directed towards national and regional capacity building, technology transfer on mutually agreed terms, cooperation in R&D programmes and exchange of know-how.

f) While all existing financial mechanisms should be fully exploited, a thorough review of their adequacy in meeting the challenges of ICT for development should be completed by the end of December 2004. This review shall be conducted by a Task Force under the auspices of the Secretary-General of the United Nations and submitted for consideration to the second phase of this summit. Based on the conclusion of the review, improvements and innovations of financing mechanisms will be considered including the effectiveness, the feasibility and the creation of a voluntary Digital Solidarity Fund, as mentioned in the Declaration of Principles.

g) Countries should consider establishing national mechanisms to achieve universal access in both underserved rural and urban areas, in order to bridge the digital divide.

E) Follow-up and evaluation

28. A realistic international performance evaluation and benchmarking (both qualitative and quantitative), through comparable statistical indicators and research results, should be developed to follow up the implementation of the objectives, goals and targets in the Plan of Action, taking into account different national circumstances.

a) In cooperation with each country concerned, develop and launch a composite ICT Development (Digital Opportunity) Index. It could be published annually, or every two years, in an ICT Development Report. The index could show the statistics while the report would present analytical work on policies and their implementation, depending on national circumstances, including gender analysis.

b) Appropriate indicators and benchmarking, including community connectivity indicators, should clarify the magnitude of the digital divide, in both its domestic and international dimensions, and keep it under regular assessment, and tracking global progress in the use of ICTs to achieve internationally agreed development goals, including those of the Millennium Declaration.

c) International and regional organizations should assess and report regularly on universal accessibility of nations to ICTs, with the aim of

creating equitable opportunities for the growth of ICT sectors of developing countries.

d) Gender-specific indicators on ICT use and needs should be developed, and measurable performance indicators should be identified to assess the impact of funded ICT projects on the lives of women and girls.

e) Develop and launch a website on best practices and success stories, based on a compilation of contributions from all stakeholders, in a concise, accessible and compelling format, following the internationally-recognized web accessibility standards. The website could be periodically updated and turned into a permanent experience-sharing exercise.

f) All countries and regions should develop tools so as to provide statistical information on the Information Society, with basic indicators and analysis of its key dimensions. Priority should be given to setting up coherent and internationally comparable indicator systems, taking into account different levels of development.

F) Towards WSIS phase 2 (Tunis)

29. Recalling General Assembly Resolution 56/183 and taking into account the outcome of the Geneva phase of the WSIS, a preparatory meeting will be held in the first half of 2004 to review those issues of the Information Society which should form the focus of the Tunis phase of the WSIS and to agree on the structure of the preparatory process for the second phase. In line with the decision of this Summit concerning its Tunis phase, the second phase of the WSIS should consider, *inter alia*:

a) Elaboration of final appropriate documents based on the outcome of the Geneva phase of the WSIS with a view to consolidating the process of building a global Information Society, and reducing the Digital Divide and transforming it into digital opportunities.

b) Follow-up and implementation of the Geneva Plan of Action at national, regional and international levels, including the United Nations system, as part of an integrated and coordinated approach, calling upon the participation of all relevant stakeholders. This should take place, *inter alia*, through partnerships among stakeholders

CHAPTER XV

SEMI CONDUCTOR ACT

Immediately after the Information Technology Act 2000 was passed in the Indian Parliament, yet another law which has an indirect impact on Cyber space was passed by the Parliament. This was the Semiconductor Integrated Circuits Layout Design Act 2000. (SCA-2000).

This was a piece of legislation following India becoming a signatory to the TRIPS (Trade Related Aspects of Intellectual Property Rights) agreement between UN member nations.

The Act received the assent of the President on the 4th September 2000. At present the rules under the Act are being finalized. Even though a detailed discussion of this Act is not within the scope of this book, a bird's eye view of the Act is provided here so as to create an awareness amongst the readers about this Act.

The SCA-2000 provides for registration of Integrated Circuit Layouts and confers certain rights on the creator of the design similar to Copyright.

According to the Act, "layout-design" means a layout of transistors and other circuitry elements and includes lead wires connecting such elements and expressed in any manner in a semiconductor integrated circuit .

"Semiconductor integrated circuit" means a product having transistors and other circuitry elements which are inseparably formed on a semiconductor material or an insulating material or

inside the semiconductor material and designed to perform an electronic circuitry function.

This definition includes "Chips" that are used in a Computer and also many other electronic devices such as the Washing Machines, Microwave Ovens, Mobile phones, Smart Cards etc.

It is these chips that create the "Cyber Space" of communication between different hardware pieces. These are the Chips that form the brains of the automated Computer systems that are part of the Cyber society.

The objective of the Act is to provide a means for protecting the Intellectual Property involved in such circuit design and enabling the owner to assign or transfer the right for consideration by means of royalty or otherwise.

Any "Original" and "Distinctive" circuit designs which have not been commercially exploited in India or elsewhere, can be registered under this Act with a registrar to be appointed for the purpose.

Unlike the "Patent" which can be registered only by an inventor and Copyright which belongs to the "Author", the Act prescribes that where an original layout-design has been created in execution of a commission or a contract of employment, the right of registration to such layout-design under this Act shall belong, in the absence of any contractual provision to the contrary, to the person who commissioned the work or to the employer.

There is a provision for registering a design jointly in the names of more than one person if the right is indistinguishable.

The registration will be valid for 10 years. Any act of reproducing, whether by incorporating in a semiconductor integrated circuit or otherwise, a registered layout-design in its entirety or any part thereof, by any person other than the registrant or his assignee will constitute "Infringement" and provides a right to the registrant to proceed against such a person.

Any act of importing or selling or otherwise distributing for commercial purposes a registered layout-design or a semiconductor integrated circuit incorporating such registered layout-design or an article incorporating such a semiconductor integrated circuit containing such registered layout-design for the use of which such person is not entitled under this Act will also be an infringement of the rights of the registrant.

There is a "Fair Use" kind of provision which allows reproduction where such act is performed for the limited purposes of scientific evaluation, analysis, research or teaching and which will not constitute act of infringement within the meaning of this Act.

Where any person by application of independent intellect has created a layout-design which is identical to a registered layout-design, then, any act of such person in respect of the layout-design so created shall not be the infringement of the registered layout-design.

OFFENCES UNDER SCA-2000

There are both Civil and Criminal remedies provided in the SCA-2000 against violations of the provisions of the Act.

Any person who knowingly and willfully infringes the rights of a registrant of a lay out design is punishable with imprisonment for

a term which may extend to three years, or with fine which shall not be less than fifty-thousand rupees but which may extend to ten lakhs rupees, or with both.

Where a person is convicted of an offence of infringement, the Court convicting him may direct the forfeiture to Government of all goods and things by means of, or in relation to which the offence has been committed.

Any person who falsely represents an unregistered design as registered, is punishable with imprisonment for a term which may extend to six months, or with fine which may extend to fifty thousand rupees or with both.

If the person committing an offence under this Act is a company, the company as well as every person in charge of, and responsible to, the company for the conduct of its business at the time of the commission of the offence shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

In any prosecution under this Act, the Court may order such costs to be paid by the accused to the complainant, or by the complainant to the accused, as the court deems reasonable, having regard to all the circumstances of the case and the conduct of the parties. Costs so awarded shall be recoverable as if they were a fine.

The Act envisages constitution of an Appellate Board called the Layout-Design Appellate Board to redress some of the grievances arising out of the registration of design layouts. The Appellate Board shall consist of a Chairperson, Vice-Chairperson, and such other Members as the Central Government may deem fit.

The Appellate Board will hear the appeals against any of the decisions of the registrar. It will also determine the royalty payable to the registered owner of a design in cases such as the user had no prior knowledge of the registration and had proceeded to use the same in good faith. It will also rectify the register of Layout designs when necessary and will have the power to cancel the registration in certain cases.

The board also has powers to permit the use of a registered layout design without the authorization of the registered proprietor for non-commercial public purposes or for the purposes relating to national emergency or of extreme public urgency for a limited period. While granting such compulsory license, the Board will fix the royalty payable to the registered proprietor of the design.

An order or decision made by the Appellate Board is executable by a Civil Court having local jurisdiction as if it were a decree made by that court.

Thus the SCA-2000 is a law which has a blend of "Patent Act" and "Copyright Act" and applies to the intellectual property concerning the hardware that constitutes part of the Cyber World.

CHAPTER XVI

COMMUNICATION CONVERGENCE BILL

[Ed: The Bill has since been Withdrawn from the Parliament. However, since the contents of this Chapter are conceptually relevant to the study of Cyber Laws and also there is a possibility of the Bill being reintroduced, thischapter has been retained]

WHAT IS CONVERGENCE?

Internet is a technology which has many dimensions. It is a "Information Superhighway" to some and a "Communication Device" to another. It is a "Shopping Mall" to some and an "Education Center" for another. In this multifaceted nature of the Internet we see a "Convergence" of different consumer needs.

Similarly, if we look at the gadget called "Computer", it is no longer only a "Computing Tool". It is today a "Secretary", a "Multi Media Communication Device" or simply an "Internet Access Tool" which is everything from information to shopping etc.. This changing perception of the Computer is a reflection of the "Convergence of Technologies" that is happening around us.

The technology behind transmission of Voice and Images from the producer to the distributor and on to the consumer has changed with the digitization of Voice and Images. The specialized Voice and Image receiving tools such as the Telephone and the TV now are substituted by more versatile devices including Computers. In some cases the devices themselves are being embedded with computer chips so that they become special purpose computers.

At the industry end, the production and distribution of Voice and Image has undergone an even more perceptible change with the digital technology being used for Internet, Telecommunication and Broadcasting on a common backbone.

BAND WIDTH BRINGS THE TRANSITION

One of the important reasons which has lead to the acceleration of convergence is the increasing bandwidth available for data transmission. It was not long ago that the modems migrated from 9600 bits per second (bps) to 14400 bps. It has since jumped to 33.6 kbps and onto 56 kbps. In many places we now see 64 kbps lease lines, ISDN lines as well as the new technology "DSL" connections. The "Cable" modem promises to increase the bandwidth even further.

Even while the last mile connectivity (between the consumer and the nearest ISP) has grown from 9.6 KB to 64 KB, the backbone supporting the networks on optical fiber has taken the backbone bandwidths to terra-bits (Million Million bits) level.

When the band width of Internet connectivity was low, the audio and video files were difficult to be transmitted particularly for an "online experience". As higher and higher bandwidth became available for Internet, the transmission of Sound and Video files became feasible in real time.

As a result, multimedia content could be easily delivered across the Internet either as a part of a web site design or as a product or service. Coupled with the technological innovations which can "Compress" audio and video files to smaller size without loss of quality, it has become possible today to send streaming audio and streaming video as a part of web content. These developments

have blurred the difference between the different communication media namely the "Data", "Voice" and "Picture".

Traditionally, Voice Telephony, Radio, TV Broadcasting, and On-line computer services were distinct services. They operated on different networks and used different "Platforms" namely Telephones, Radio Sets, TV sets, and Computers. They entered the market at different points of time and were regulated by different laws and different regulators, usually at national level. But with the "Convergence" of these media, there is now an overlapping of regulations requiring a new look at the legal regime. The area of operation has also grown beyond the national boundaries and created problems in interpretation of law and its enforcement.

The technical convergence of the media brought about by digital transmissions at high bandwidth has also changed the perspective of the business organizations. Today a data network owner thinks of using the network for telephony while the TV transmission company thinks of using the content on the web.

Telecommunications, Media and IT companies are therefore using the flexibility of digital technologies to offer services outside their traditional business sectors, increasingly on an international or global scale.

The emerging "Convergence Laws" will have to therefore cater to the requirements of all the three industries namely the IT, Media and Telecom.

INTERNET TELEPHONY

Initially, Internet took over the "Fax" system and "Fax Servers" started relaying fax messages over data net works. Today the

technology for Voice over IP is available to any one with an Internet connection and a Computer. Facilities such as Net2phone, Dialpad, Phonefree, Firetalk etc offer easy to use software to carry voice over Internet. Many hardware devices are also in the market today which when installed on the motherboard, converts the Computer into a telephone exchange where a call to any part of the globe would cost only as much as the local call.

Understanding the difficulties arising out of archaic laws the Indian Government took the bold step of making Internet telephony legal with effect from April 1, 2002 through an administrative guideline. Accordingly, long distance international calls can now be made from a computer to another computer as well as from a Computer to a telephone abroad.

Computer to Telephone interface is provided as a special service by the ISP at a cost which is of course a fraction of the normal telephone costs. Many of the ISP s such as SIFY and Net4India have already launched their international long distance Computer to telephone services.

The permission for Internet telephony does not however extend to Computer to Telephone within India which is still not permitted.

ISP s have also been permitted to use VOIP (Voice over Internet Protocol) technology for transmission of voice files over the internet backbone thus recognizing the "Convergence" aspect.

THIS IS THE BEGINNING OF THE CONVERGENCE LAWS

Making Internet Telephony legal was just the first step towards bringing in Convergence Laws. The problems which lead to making of Internet telephony legal has also surfaced in other areas.

The TV broadcast channels are now finding that multimedia broadcast over Internet is cheaper and perhaps more customer friendly. Given an option, People would opt to watch their favourite programme on demand over the Internet rather than on the conventional TV. This could however affect the economics of TV broadcasting. The Challenge before the legal administrators is to balance the aspirations of the new generation to whom technology is bringing in benefits which were not contemplated earlier, with the need to protect existing industries and legal commitments of Governments.

OWNERSHIP OF CONTENT

In the convergent era, Content produced for one media becomes available for distribution through other media as well. Before the advent of Internet, the rights on a movie would be discussed and settled only for distribution through theaters. The rights of a Book would be discussed only with reference to publishing in print. Probably most of the contracts spoke of "All Rights for Distribution/Publication by whatever means" and the originator had no idea that one day the market on the Internet would be bigger than the traditional media such as theaters for the movie or print for the book. The music CD industry has realized at a great cost that music can not only be distributed through the CD but also through the Internet using a "File Sharing Technology".

Event management people have also realized that today it is not enough to obtain the broadcast rights for the Cricket World Cup on the TV but it is also important to capture the rights for the Internet both for web casting and carrying of scores over a "Ticker bar on the website".

Just as the convergence has given raise to many complications in the Copyright issue, soon we may find conflicts in the "Patent area" also. It may be possible that a patented web process is allegedly infringed through a media innovation. The innovator may however contest this as an "Improvement" outside the imagination of the original Patent holder.

THE FUTURE SCENARIO

Thus the Convergence phenomenon will give raise to many issues in the IPR area which are not easy to resolve. Just as we have highlighted the problems in resolving the disputes between the Trade Mark and Domain Name issues, some instances of Copyright and Patent infringement will create a clash between "Development" and "Protection".

The maturity of the legislators will therefore be put to test in defining the legal regime that would let the different media grow independently and collectively.

Since the Convergence laws tend to find a common meeting point for the very highly regulated Telecom industry, the highly regulated broadcasting industry and the sparsely regulated Information technology industry, there will be some loss of freedom for the IT industry while there would be some relief for the other two regulated industries. Achieving a fine balance between the stake holders in these three industries while bringing

a common legislation will therefore be the most important aspect of such a legislation.

In order to address these issues, a comprehensive legislation in the form of Communication Convergence Bill (CCB) is being sought to be passed in India. The bill has been referred to a select parliament committee and can become law any time. Already the Ministries of Telecommunications and Information Technology have been merged and sooner or later the Ministry of Information and Broadcasting would also be merged with them to form the Ministry for Convergence Economy.

In the following paragraphs, we shall take a journey of the Bill and understand its salient features.

THE OBJECTIVES OF CCA

Basic objectives of this Act are to establish a unified regulatory framework for carriage and content of communication in the scenario of convergence of telecommunications, broadcasting, data-communication, multimedia and other related technologies and services.

It seeks to establish the powers, procedures and functions of a single regulatory and licensing authority and of the Appellate Tribunal.

Convergence in this context means convergence of mediums or technologies facilitating provision of all services by using a given facility or network and vice versa.

It also means convergence of services at the provider's end as well as the consumer's end, meaning, thereby, a service provider

should be able to provide a whole range of technologically feasible services and a consumer should be able to receive all services through a given terminal at any time and place of his choice.

The Act aims at

-facilitating development of national infrastructure for an information based society, and to enable access thereto;

-providing a choice of services to the people with a view to promoting plurality of news, views and information

The scope of regulation envisaged in the CCA covers

Frequency Spectrum Management
Licensing
Tariff Management
Content Regulation
Crimes and Punishment

The Act however is not applicable to the facilities or communication services owned, and operated by the Central Government or any State Government for their own use.

REPEALMENT OF ACTS

In order to remove the hurdles arising out of past legislations, the CCA will repeal the earlier legislations such as

1.The Indian Telegraph Act, 1885
2.The Indian Wireless Telegraphy Act 1933,
3.Telegraph Wire Unlawful Possession Act, 1950,
4.Cable Television Networks (Regulation) Act 1995 and
5.The Telecom Regulatory Authority of India Act, 1997.

After the CCB was drafted, the Cable Television Networks (Regulation) Act has been amended with Cable TV Network Amendment Act 2002 to make provision for the Conditional

Access System. In the final draft of the Convergence Act, this amendment Act may also have to be repealed and necessary changes incorporated in the main CCB itself.

In addition to the repealment of specific acts, the provisions of Communication Convergence Act will take effect notwithstanding anything inconsistent or contrary therewith contained in any other law for the time being in force.

THE COMMUNICATION CONVERGENCE COMMISSION (CCC)

The Act proposes setting up an autonomous body to be known as Communications Convergence Commission of India with wide ranging powers, duties and functions.

The head office of the proposed Commission will be located at Delhi, and its regional offices will be located at Kolkata, Chennai and Mumbai.

The commission will be the apex authority for all matters in connection with the Act including Licensing, Tariff Management, Content Regulation, Dispute Resolution etc.

It will be assisted by Adjudicators and an Appellate tribunal in discharging its dispute resolution functions.

The actions of the Commission are subject to appeal with the Supreme Court of India only.

SPECTRUM MANAGEMENT COMMITTEE

The Central Government will also establish, by notification, a Spectrum Management Committee with the Cabinet Secretary as its Chairman and consisting of such other members as may be

notified by it from time to time to deal with all matters concerning management of the "Frequency Spectrum" which is a scarce global resource.

The Committee would coordinate with national and international agencies for allocation of available spectrum for strategic and non-strategic or commercial purposes.

The Wireless Advisor to the Government of India will be designated as the Spectrum Manager, and act as Member-Secretary of the Spectrum Management Committee.

The CCC shall be responsible for assignment of the non strategic and commercial spectrum to various users but the Act mandates that the CCB shall assign frequencies only with the prior approval of the Spectrum Management Committee.

COMPOSITION OF THE CCC

The Commission will be a body corporate having perpetual succession and a common seal with power to acquire, hold and dispose of property, both movable and immovable and to enter into contracts. It can sue and be sued in its own name.

The Commission will consist of a Chairperson, not more than ten Members and the Spectrum Manager as an ex-officio Member.

The Chairperson as well as not less than six Members, (other than the ex-officio Member), will be whole-time Members and the remaining will be part time Members.

The chairperson and Members, other than the ex-officio Member, shall be appointed by the Central government from amongst

persons of eminence recommended by a Search Committee from fields such as literature, performing arts, media, culture, telecommunications, law, broadcasting technology, information technology, finance etc.

The Chairperson of the Appellate Tribunal shall be a person who is, or has been, a judge of the Supreme Court and shall be appointed in consultation with the Chief Justice of India.

The Chairperson and whole-time Members will hold office for a term of five years or until they attain age of 65 years whichever is earlier. They will not be eligible for re-appointment.

FUNCTIONING OF THE CCC

The Act has prescribed a set of objectives for the commission derived from the objectives of the Act itself.

They are,

(i) the communication sector is developed in a competitive environment and in consumer interest;

(ii) communication services are made available at affordable cost to all especially uncovered areas including the rural, remote, hilly and tribal areas;

(iii)there is increasing access to information for greater empowerment of citizens and towards economic development;

(iv) quality, plurality, diversity and choice of services are promoted;

(v) a modern and effective communication infrastructure is established taking into account the convergence of information technology, media, telecom and consumer electronics;

(vi) defense and security interests of the country are fully protected;

(vii) introduction of new technologies, investment in services and infrastructure, and maximization of communications facilities and services (including telephone density) are encouraged;

(viii)equitable, non-discriminatory interconnection across various networks are promoted;

(ix)licensing and registration criteria are transparent and made known to the public;

(x)an open licensing policy allowing any number of new entrants (except in specific cases constrained by limited resources such as the spectrum) is promoted; and

(xi) the principle of a level playing field for all operators, including existing operators on the date of commencement of the Act, is promoted so as to serve consumer interest.

It may be observed from the above that the objectives are both "Regulatory" and "Developmental". They are meant to protect "Consumer interest" as well as "Commercial interests". They are also meant to protect both "Governmental interests" as well as "Private sector interests".

These mutually conflicting interests will test the ingenuity and commitment of the CCC in the days to come if it has to live up to the expectations prescribed here in.

Amongst the specific duties envisaged for the Commission are,

(i) Carry out management, planning and monitoring of the spectrum for non-strategic/ commercial usages

(ii) grant licenses for purposes of the Act, and determine and enforce license conditions and determine fees (including fees for usage of spectrum) wherever required;

(iii) determine appropriate tariffs and rates for licensed services, wherever considered necessary and keeping in view the objectives and guiding principles in the Act .;

(iv) ensure that the grant of licenses will not result in eliminating competition or in one or more service providers becoming dominant to the

detriment of other service providers or consumers; .

(v) promote competition and efficiency in the operation of communication services and network infrastructure facilities;

(vi) formulate and determine conditions for fair, equitable and nondiscriminatory access to a network infrastructure facility or network service such other related matters in respect thereof; .

(vii) take measures to protect consumer interests and promote and enforce universal service obligations; .

(viii) formulate and lay down programme and advertising codes in respect of content application services;

(ix) formulate and lay down commercial codes in respect of communication services and network infrastructure facilities;

(x) take steps to regulate or curtail the harmful and illegal content on the internet and other communication services; .

(xi) formulate and lay down codes and technical standards and norms to ensure quality and interoperability of services and network infrastructure facilities (including equipment); .

(xii) carry out any study and publish findings on matters of importance to the consumers, service providers and the communications industry;

(xiii) institutionalize appropriate mechanisms and interact on a continual basis with all sectors of industry and consumers, so as to facilitate and promote the basic objectives of the Act; to encourage self regulatory codes and standards;

(xiv) report and make recommendations on such matters as may be referred to it by the Central Government;

(xvi) report and make recommendations either suo moto or on such matters as may be referred to by the Central Government in the matter prescribed

(xvi) perform all or any functions in furtherance of the objects of this Act, or such as may be prescribed.

It may again be observed that many of the duties prescribed have inherent conflicts and managing them to the satisfaction of the community will be a challenge to the Commission.

Given the experiences of TRAI in the field of tariff fixation, it appears that balancing the consumer needs with various industry requirements will be an onerous task and is likely to lead to controversies and litigations.

LICENSING

Licensing is obviously one of the prime duties of the CCC and will be the tool through which the objectives are set to be achieved.

The licensees who are operating under the provisions of the laws that have been repealed by the CCB such as the Telegraph Act, Wireless Act, TRAI Act, Cable Television Act etc will be required to make a fresh application for license within 6 months of the Act coming into force with the appropriate authority under the new Act. Until the license is renewed, the terms of the earlier license will however continue.

Apart from the wireless devices, possession of which need license for possession, the CCC will now license business in the following five categories.

- Network infrastructure facilities.
- Network Services
- Application Service
- Content Application Service
- Value Added Network Application Service.

For the purposes of licensing, Network infrastructure facilities includes earth station, cable infrastructure, wireless equipments, towers, posts, ducts and pits used in conjunction with other communication infrastructure, and distribution facilities including facilities for broadcasting distribution.
Networking services includes band-width services, fixed links and mobile links.

Network application services includes public switched telephony, public cellular telephony, global mobile personal communication by satellite, internet protocol telephony, radio paging services, public mobile radio trunking services, public switched data services and broadcasting (radio or television service excluding continued).

Content application services includes satellite broadcasting, subscription broadcasting, terrestrial free to air television broadcasting and terrestrial radio broadcasting;

Value added network application services includes internet services and unified messaging services excluding information technology enabled services such as call centers, electronic-commerce ,tele-banking ,tele-education, tele-trading ,tele-medicine, videotext and video conferencing shall not be licensed under this Act.

CONTENT CODES

One of the features of the CCA which has come in for criticism has been an attempt to prescribe codes and standards for Content.
According to the Act, the Commission will by regulations from time to time specify programme codes and standards to ensure

(i) that nothing is contained in any programme which is prejudicial to the interests of the sovereignty and integrity of India, the security of State, friendly relations with foreign States, public order or which may constitute contempt of court, defamation or incitement to an offence. ; .

(ii)that fairness and impartiality in presentation of news and other programmes.
(iii) emphasis on promotion of Indian culture, values of national integration, religious and communal harmony, and a scientific temper.

(iv) decency in portrayal of women, and restraint in portrayal of violence and sexual conduct in all programmes.

(v) enhancement of general standards of good taste, decency and morality.

(vi) avoidance of offence to religious views and belief; and

(vii) prevention of unjust and unfair treatment in any programme, and unwarranted infringement of privacy in or in connection with, obtaining of material included in such programme.

This section obviously means that the Commission will not only be able to exercise its censorship rights on content which is considered objectionable, but also prevent unfair means of obtaining content of the type perhaps used in the Tehelka.com controversy. Some have criticized this section as an attempt at "Moral Policing".

While the possibilities of misuse of this section cannot be ruled out, its relevance cannot also be undermined. Whether the apprehensions of the critics will be vindicated or proved unfounded will depend on how the Commission plans to implement this portion of the regulation.

Amongst the powers that the Commission has reserved is one regarding compulsory live broadcasting rights for any important event that happens in India.

According to the Act, the Central Government may notify in advance any event of general public interest to be held in India, shall have to be carried on the network of the public broadcaster as well.

This means that if world cup cricket happens in India and Star TV has the exclusive rights for broadcast, the Government can mandate that the coverage must be carried on the Doordarshan as well.

We may recall that in a recent Mini World Cup Cricket tournament in Sri Lanka, the Government owned Sri Lankan Broadcasting Corporation faced a legal battle with the sponsors of the tournament for its right to broadcast Cricket commentary over the radio. This incident vindicates the need for the said provision in CCB.

OFFENCES AND CRIMES UNDER COMMUNICATION CONVERGENCE ACT

The Communication Convergence Act deals with both Civil and Criminal liabilities arising out of the violation of any of the provisions of the Act.

In general, monetary damages provided for in the Act are huge and range up to Rs 50 crores.

Imprisonment in terms of some of the offences may go up to 7 years.

Different types of offences dealt with are as follows:

Breach of terms and conditions of licenses, etc.

In any case of breach of any of the terms of the license or registration or failure to comply with any decision, direction or order of the Commission the commission may suspend or cancel the license and initiate adjudication proceedings for compensation.

The Commission may also order seizure of equipments used and for this purpose the authorize any District Magistrate, or Sub-Divisional Magistrate in any area ,or any other officer of the Central Government or State Government or Union territory Administration , to implement and ensure compliance of its directions and orders.

Contravention of the provision relating to transmission etc.

If any person transmits or distributes any communication or performs any service incidental thereto, by the use of a network infrastructure facility, communication service or wireless equipment which is required to be licensed or registered under this Act and not so licensed or registered, such person will be liable to a civil liability.

Delivery of content through facilities, services or equipments not licensed or registered.

If any person delivers any content for transmission or accepts delivery of any content sent by the use of network infrastructure facility, communication service or wireless equipment knowing that such facility has been established or maintained without a

license or registration or in contravention of the provisions of this Act shall be liable to a civil liability.

It may be noted that this violation includes "Acceptance of Delivery" of any content. This means that the consumers can also be made liable under this Act for receiving service from unlicensed operators. Such operators can be telephone service operators or cable TV operators.

Registration of Agreements

The Act mandates that some of the agreements entered into by the service providers with some stake holders has to be registered with the commission. If a service provider fails in this regard, he may incur civil liability under the Act. Shareholders or promoters agreements and interconnectivity agreements come under the category of such agreements requiring registration.

Failure to comply with the decision, direction or orders of the Commission.

If any person willfully fails to comply with any decision, direction or order of the Commission, he will be liable to civil liabilities under the Act.

Damage to Infrastructure Facilities:

If any person damages, displaces or destroys any cable or any part of the network infrastructure facility laid, established or place in accordance with the provisions of this Act, or if the communication services by reason of the damage or displacement so caused is interrupted, such person will be liable, -

-where the act is willful and deliberate, to a civil liability which may extend to rupees five crores and where the actual loss or damage caused is more than rupees five crores then the civil liability up to the extent of damage.

- where the act is not willful or deliberate, a civil liability not exceeding the actual loss or damage caused.

Penalty imposed under any of the above cases unless otherwise mentioned, may extend up to a maximum of Rs 50 Crores.

The Adjudicating Officer is however expected to adjudge the liability having due regard to the provisions of this Act, and also to the factors such as the actual loss, repetitive nature of the default, unfair advantage gained etc.

OFFENCES OF CRIMINAL NATURE

Running a Service without License:

Any person who, without a license, owns or provides any network infrastructure facility or provides any communication service or knowingly assists in the transmissions or distribution of such service in any manner including collection of subscription for his principal; or issuing of advertisements to such service; or dealing in, or distribution of, equipment for decoding programme, may be punishable with imprisonment which may extend to five years, or with fine which may extend to five crore rupees, or with both,.

For the second offence, the fine may extend to ten crore rupees.

Diversion of Signals:

Any person who without the permission of the service provider and with the intent to defraud, diverts any signal or decodes any content or deals in decoding equipment for such purpose may be punishable with imprisonment which may extend to five years and with fine which may extend to five crore rupees or with both and, for the second or subsequent offence with fine which may extend to ten crore rupees.

Benefiting from Unauthorized Diversion

Any person who, knowingly benefits from any unauthorized diversion or tampering with any communication service or network infrastructure facility with the knowledge that such service or facility is unauthorized or tampered, may be punished with imprisonment for a term which may extend to two years, or with fine which may extend to rupees two crores, or with both.
This may apply to an unauthorized Cable TV connection too.

Abetment for Unauthorized Diversion:

Any person who, abets or induces the making of any unauthorized diversion or tampering with any communication service or network infrastructure facility may be punished with imprisonment for a term which may extend to two years, or with fine which may extend to rupees two crores or with both

Unauthorized Interception of Communication:

Any person, who intercepts any communication or causes any communication to be intercepted or discloses to any person, any content shall be punishable with imprisonment which may extend to five years or with fine which may extend up to ten lakh rupees,

and, for a second and subsequent offence, with fine which may extend up to fifty lakh rupees.

The provisions regarding offences contained in the CCA will not affect the provision of section 69 of the Information Technology Act, 2000.

Possession of wireless equipment etc without license

Any person, who possesses any wireless equipment in contravention of the provisions of the Act or uses a radio frequency which he is not authorized to use under this Act, may be punished with imprisonment which may extend to three years or with fine which may extend to rupees two crores, or with both.

For the purpose of this section it is clarified that "radio frequencies" means any frequency of electro-magnetic waves up to and including a frequency of 3000 giga hertz.

Sending obscene or offensive messages

Any person who sends, by means of a communication service or a network infrastructure facility, any content that is grossly offensive or of an indecent obscene or menacing character; or for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, any content that he knows to be false or persistently makes use for that purpose of a communication service or a network infrastructure facility, may be punishable with imprisonment which may extend up to three years or with fine which may extend to rupees two crores or with both.

While this section partly overlaps with section 67 of the ITA-2000, it extends to other misuses of E-mails and websites

including "Spamming", "Stalking" "Defamation", "Abuse", "Hate Sites" etc which were offences not covered by ITA-2000.

Interception of communication and safeguards.

Subject to the prescribed safeguard, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government, on the occurrence of any public emergency or in the interests of the security, sovereignty and integrity of India, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, may direct:

> (i) any agency of that Government to intercept any communication on any network facilities or services; .
>
> (ii) any service provider that any content brought for communication by or communicated or received by, him shall not be communicated or shall be intercepted or detained or shall be disclosed to that Government or its agency authorized in this behalf:

The service provider shall, when called upon by any agency, which has been directed to carry out interception, extend all facilities and technical assistance for interception of the content of communication.

Any service provider who fails to assist the agency shall be punished with imprisonment for a term, which may extend to seven years.

Repetitive Crimes:

Any person who, having already been convicted of an offence may on every such subsequent conviction, be punished with imprisonment for a term which may not be less than six months

but which may extend to five years, and with fine which may extend to rupees five crores.

Attempt to commit offences

The Act provides that whoever attempts to commit or abets the commission of any offence, may be punished with the punishment provided for that offence.

Offences by companies

Where an offence under this Act has been committed by a Company every person who at the time of the offence 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 deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

However, the person will not be held liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

At the same time, where any offence under this Act has been committed by a company and it is proved that the offence has been committed 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 be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

OFFENCES TO BE COGNIZABLE

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 every offence punishable under this Act will be considered cognizable.

AUTHORITY TO SEARCH AND SEIZE

Any officer authorized by the Central Government or the Commission in this behalf may search any building, vehicle, vessel or place in which he has reason to believe that any wireless equipment in respect of which an offence has been committed is kept or concealed and take possession thereof.

DISPUTE RESOLUTION UNDER THE COMMUNICATION CONVERGENCE ACT

The Dispute resolution under the Communication Convergence Act will be handled at three levels before it passes out of the system.

Firstly, the Communication Convergence Commission itself is a quasi judicial authority and is responsible for many of the decisions particularly regarding licensing.

The Commission can appoint an "Adjudicating Officer" in cases where civil liabilities are to be determined.

Thirdly, in order to hear the appeals against the orders of the CCC and the Adjudicating officer, an Appellate Tribunal is constituted.

Any appeals against the decisions of the appellate tribunal passes on to the Supreme Court of India.

DISPUTE RESOLUTION RESPONSIBILITIES OF CCC

The CCC will decide on disputes between two or more service providers on issues relating to spectrum interference, interconnectivity, denial of fair access and practices restrictive of fair competition.

It may also take for resolution disputes between a service provider and a group of consumers or any other disputes arising out of enforcement of any provision of this Act.

It can hear any complaint and if refer the matter for adjudication.

LEGAL STATUS OF THE CCC

The Commission will have, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, for the purposes of discharging its functions under this Act.

Every proceeding before the Commission will be deemed to be judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196, of the Indian Penal Code and the Commission shall be deemed to be a civil court for the purposes of sections 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

As regards the procedures, the Commission will not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but will be guided by the principles of natural justice and, will have powers to regulate its own procedure.

ADJUDICATING OFFICER

For the purpose of adjudging whether any person has contravened any of the provisions of this Act, any rules, regulations, made there under or directions or orders issued under this act is liable to a civil liability under this Chapter, the Commission will appoint by general or special order, an officer of the commission as Adjudicating Officer for holding an inquiry in the manner provided in the Act.

If the Adjudicating Officer, after giving a reasonable opportunity for making a representation in the matter is satisfied that the person has committed any contravention, he may order the liability to.

For the purpose of discharging his powers and functions, every Adjudicating officers will have the same powers as are vested in a civil court under the code of Civil procedure, 1908.

Any proceeding before the Adjudicating Officer will be deemed as a judicial proceeding within the meaning of sections 193 and 228, and for the purpose of sections 196, of the Indian Penal Code and the Adjudicating Officer shall be deemed to be a civil court for the purpose of section 195 and chapter XXXVI of the Code of Criminal Procedure, 1973.

COMMUNICATIONS APPELLATE TRIBUNAL (CAT)

The Central Government shall, by notification, establish an Appellate Tribunal to be known as the Communications Appellate Tribunal, to exercise the jurisdiction, powers and authority conferred on it by or under this Act.

The CAT is a multi member tribunal and will consist of a Chairperson and not more than six Members to be appointed, by notification, by the Central Government. The appointment of Chairperson and Members of the Appellate Tribunal will be made by the Central Government in consultation with the Chief Justice of India.

The CAT will function through benches that will be constituted by the Chair person at Delhi and such other places as may be notified. Each such bench will be presided over by a member of the CAT who has been a judge of the High Court and will consist of two or more members. The Central Government will also notify the jurisdiction of such tribunals.

Any person aggrieved by any decision or order of the Commission may prefer an appeal to the Appellate Tribunal.

The Appellate Tribunal shall have, for the purpose of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure,1908.

Every proceeding before the Appellate Tribunal will be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196, of the Indian Penal Code.

It will also be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973The CAT is not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and will have powers to regulate its own procedure..

An order passed by the Appellate Tribunal under this Act will be executable by the Appellate Tribunal as a decree of a civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

A complaint may be filed before the Commission alleging that a service provider or any other person has incurred a liability to a civil liability under the Act..

Any appeal against the orders of the CAT will lie with the Supreme Court. Also the Act provides that The Act provides that no court inferior to that of a Court of Session may try an offence under this Act.

RECOVERY OF CIVIL LIABILITIES

The CCA categorically provides that without prejudice to other modes of recovery, any civil liability imposed under this Act if not paid, be recovered as an arrear of land revenue and the Commission shall be empowered to suspend the license or registration of the person on whom the civil liability is imposed till the same is not paid.

JURISDICTION OF CIVIL COURTS

No civil court will have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer or the Appellate Tribunal or the Commission 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.

The Commission may, by order in writing, authorize any District Magistrate or Sub-Divisional Magistrate in any area or any other officer of the Central Government or State Government or Union territory Administration to implement and ensure compliance of its directions and orders; and when so directed or authorized, such Magistrate or officer shall be bound to implement and carry out such directions and orders.

The CCC can impose on service providers certain duties such as follows.

Duties of service providers

Every service provider shall , wherever required or applicable-

(i) give effect to Universal Service Obligations;
(ii) provide such life saving services as may be prescribed;
(iii) provide service to any person on demand within a reasonable period of time and on a non-discriminatory basis; and
(iv) follow the codes and standards laid down and specified by the Commission;

Every service provider of a content application service will endeavour to provide a suitable proportion of programme of indigenous origin; and ensure that no programme forming part of its services infringes any copyright.

Every service provider holding a license for providing distribution of broadcasting services will provide a specified number and type of broadcasting services, including those of the public service broadcaster, in such manner, as may be prescribed, include only licensed broadcasting service in his delivery package for the purposes of distribution; and use not more than such

number of channels as specified by regulations, out of the total channel capacity of the system, for providing his own programming.

RIGHT OF WAY

In any infrastructure project, one of the problems that the facility providers face is the delay in implementation of project arising due to various litigations from land owners whose land has to be acquired for the purpose of the project. Such problems often arise in Road Construction and Railway Line projects.

Since one of the important aspects of Telecommunications is the laying of Cables for transmission of signals, and such cables have to be laid all across the country and within cities and metros, legal problems of land acquisitions also confront telecommunication projects.

The CCA has addressed this issue exclusively by legislating on several aspects regarding provision of "Right of Way". This is a special right given to the facility provider under the Act to facilitate project implementation on schedule.

Accordingly, any person entitled under the provisions of CCA, to provide services or facilities (facility provider) may lay, and establish cables and erect posts under, over, along, across, in or upon any immovable property vested in or under the control or management of a public authority.

Any such public authority under whose control or management, any immovable property is vested shall, on receipt of a request from a facility provider permit the facility provider to do all or any of the following acts namely.

(a) to place and maintain underground cables or posts; and
(b) to enter on the property from time to time, in order to place, examine, repair, alter or remove such cables or posts.

The Act mandates that such permission is to be promptly given and should not be unreasonably withheld or denied.

The Act also provides that in any emergency, the facility provider may enter upon the property for even without first obtaining such permission.
If any dispute arises including refusal of permission by the public authority ,the district court within whose local limits of jurisdiction the property concerned is situated will determine the same.

Similarly, when the facility provider intends to make use of private land for constructing or laying of cables or erecting posts only he should first try to obtain the consent in writing of owner of the land or premises.

However, if in the opinion of a facility provider, consent to the reasonable use of any land is not forthcoming, he may make an application to the Commission and take such steps as the Commission directs, to use of the land or premises for constructing or laying cables or erecting posts on such terms as the Commission may deem fit. The Commission will have full powers to take a decision on the matter and fixing the compensation to be paid to the land owner.

THE CONCERNS

What strikes an observer about the CCA is that the penalties prescribed are unprecedented in the annals of the Indian

legislative history. The maximum civil liabilities extend up to Rs 50 crores. The decision on determining the quantum of the penalty rests in most cases with the "Adjudicating Officer" and the pressures on misuse of such a huge discretion would be a matter of concern to the public. There has to be adequate checks and balances to prevent any possibilities of such misuse.

Even though the large penalties have been indicated keeping in mind the Telecom sector in consideration, many of the offences mentioned in the At can very well be committed by an ordinary house hold using Cable TV. The penalties look misplaced in this context and leaves too much of a black mailing power with the Cable operator in case of minor violations.

Similarly the Content code for programmers also need to be adequately monitored during its implementation or else, it can be misapplied. We need to wait for the passing of the Act with the final amendments as well as the rules under the act to assess the exact impact of the Act. It is no doubt that Communication Convergence Act is a land mark legislation in India and needs to be watched with eagle eyes.

CHAPTER XVII

BUSINESS OPPORTUNITIES IN CYBER LAW

Whenever a new development takes place in a society, there are opportunities for the early movers and innovative businessmen to make a commercial gain out of the developments. Some of the opportunities also represent a contribution to the society while some thrive on the confusion that prevails during the transformation stage. This is as much true of software development as for Cyber Law.

Cyber Law being a fundamental law, it's impact is on the entire Cyber community. In as much as the Cyber Society impacts the real society, Cyber Laws also impact the non Cyber Community. It therefore presents many interesting business opportunities that can be harnessed by the straight minded and exploited by the crooked minded.

Let's focus more on the positive business opportunities that arise out of the passage of laws for the Cyber space.

DIGITAL SIGNATURES

One of the first business opportunities that arise out of the passage of the Information Technology Act-2000 is the business surrounding Digital Signatures.

Digital Signature is an industry which will issue Identities for large number of Netizen and Every E-Commerce Server. If we took a long term view, almost every Netizen who would like to participate in E-Commerce or E-Governance would need to hold Digital Certificates. E-Contracts. Just as people hold Credit Cards

they need to hold Digital Certificates.

It would also be necessary for people to use multiple Digital ID s for different legitimate purpose. For example, a person may need a Digital ID for his personal correspondence with his friends and his personal E-Commerce or E-Governance requirements. As an employee of an organization, his employer may provide him another digital certificate so that he can sign digital documents on behalf of his employer n his official capacity. If he holds multiple official positions such as director of different companies, he may need one digital ID for each of his official positions.

It is in fact realistic to expect that every organization would like its employees, especially those who use Intranet, Extranet or correspond with their clients on the Internet to hold Digital IDs.

Every Official of the Government who deal with the public in terms of Contracts and official notifications should have a digital ID s of their own in the official capacity.

Similarly, every E-Commerce web site needs its Server to be provided with a Digital Certificate so that it can undertake secured E-Commerce transactions.

All this means that if there are likely to be 150 lakh Netizens today in India, the current market for Digital Certificates for individuals is itself 150 lakhs and this is growing at a rate of around 30 % pa.

The current penetration of the market is near zero and a marketing professional will call this nothing short of an incredible opportunity. If we further consider that the Digital certificates are valid for specific periods and may have to be renewed from time to time, the potential of "Repeat Business" appears to be mind

boggling.

BUSINESS POTENTIAL FOR A CERTIFYING AUTHOIRITY

Looking a India in particular, the current Netizen population is expected to be around 150 lakhs today and set to grow to 250 lakhs in the next three years. Most of the Internet usage today is amongst educated professionals and the need for dual ID s as well as acceptance of the concept is likely to be significant. Assuming that the market penetration is around 10 % the total number of Digital ID holders in the next five years could reach 25 lakhs. At an average cost of Rs 1000 per year, this market would be worth Rs 250 crores per annum at the end of 5 years and is available to the Certifying Authorities who are licensed by the Controller.

Presently only two CAs have made a entry in to the field and are yet to commence aggressive marketing at retail level. Hence this entire market is available for exploitation by the 10 or 20 CA s who may be in the market in the next 5 years.

If we add the market for Server Certification which on an average costs around Rs 25,000 per year, and assume some 10,000 potential E-Commerce sites, another RS 25 crores per annum business is available for the picking.

BUSINESS POTENTIAL FOR CA ANCILLARY SERVICES

Out of the gross revenue of Rs 275 crores per annum expected to be generated by the CA s, at least an amount of Rs 200 crores would be reinvested by them in the support industries such as the Infrastructure providers for CA business, as well as in Personnel costs, Marketing and Advertising. These are potential business opportunities for those industries.

BUSINESS POTENTIAL FOR CHARTERED ACCOUNTANTS AND IT SECURITY SPECIALISTS

The need to set up and maintain secured infrastructure for providing CA services means that security audits have to be conducted by qualified Chartered Accountants from time to time while the security specialists have to maintain round the clock vigilance on technical security of the network.

DIGITAL SIGNATURE RELATED BUSINESS POTENTIAL FOR SOFTWARE INDUSTRY

As the use of Digital Signatures grow, there will be need to further research and develop better cryptography products and integrate them into various applications. New algorithms have to be continuously developed to keep racing with those who break them.

This is a source of continuous occupation for Security Software Developers.

More over, every application has to be PKI enabled so that documents created by the applications can be digitally signed. This requires a large number of applications for PKI enabling applications. One such application will be required for each computer installed in the Country.

CYBER FORENSICS

One new area of business which is growing along with the Cyber Crimes is the "Cyber Forensics".

As the need to quickly apprehend and prosecute Cyber Criminals become important, development of special tools for Data Recovery, Crime Source Tracking, Cyber Patrolling and Vigilance, Ethical Hacking etc become necessary.

This would involve development, training of personnel and marketing of such tools which will open up a new branch of business that the IT industry has not so far explored.

BUSINESS POTNTIAL FOR LEGAL PROFESSIONALS

With more and more businesses adopting E-Way of doing business, disputes in the corporate sector will predominantly be around Electronic Documents. Every legal dispute may therefore involve Cyber Laws in some way.

Further the incidents of Cyber Crimes such as Hacking, Virus, Distributed Denial of Service etc will need to be addressed under the Cyber Laws. Once the Convergence Act comes into play, the huge sector of Telecom and Broadcasting in the convergent era will also be a subject matter of Cyber Law.

Cyber Law practice will therefore emerge as a very important specialization area for Legal Professionals. Rather than trying to estimate the potential for this industry, we can say that while "There will be No Business without E-Business", there will be "No Legal Practice without Cyber Law".

The setting up of Cyber Regulations Appellate Tribunals, Communication Convergence Commission, Communication Appellate Tribunal etc will open new Judicial entities to expand the opportunities for Legal professionals to use their Cyber Law skills.

IT TRAINING OPPORTUNITIES

There is already a move in India to set up an E-Court which will come into operation in the next few years. Even before such a development, Online Arbitration centers are already coming up in various countries and soon may find a place in India too. These will not only require Cyber Law Literate lawyers, but also development of Cyber Trained Lawyers.

This means that IT training centers can now look forward to training Lawyers on the use of Computers, Internet and related matters.

It is needless to say that the requirement of spreading the Cyber Law knowledge amongst the vast number of Netizens, Legal and Non Legal professionals, Law Teachers, Law Enforcement Officials, Judges, Government Officials etc, will provide almost an almost unlimited, perennial opportunity for Cyber Law Educationists.

SOFTWARE FOR LEGAL SECTOR

With more and more lawyers acquiring computer capabilities, some of them at least would like to improve their professional competence with the use of Computers and business software that is tailor made for their requirement.

There is a need for "Case Management" software that tracks the progress of cases, keep the clients in the information loop and ensures quick availability of documents in standardized and customizable form.

There is a need for "Data Mining" software which can locate case laws and relevant information in the volume of data that is to be sifted by an advocate to support his case apart from creating a reference source of Court Decisions.

There is also a need for "Collaboration Software" so that specialists in different disciplines can remotely contribute to the development of an argument for a case without the need for traveling and also to serve clients who have located at different parts of the Country or the Globe.

There is also a need for "Compliancy Guidelines" in the form of functional guidance software on the lines of HIPAA compliancy software.

This whole suite of software products for the legal sector and some of the Cyber Forensic software as an investigation tool will be required to be developed for the legal sector. Even the consumers, namely the litigants will be benefited by their lawyers using such software since they are likely to improve the efficiency of the lawyer's operations.

Some of the services including Online Arbitration, Trade Mark Search, Verify for Look Alikes etc will also lend themselves as IT enabled services serving a large number of people on a usage basis or otherwise.

This area of legal industry software is again a virgin area available for software industry to exploit.

In summary therefore we can say that the onset of Cyber Laws have created new doors of opportunity for several types of professionals and would make a substantial contribution to the business world.

CHAPTER XVIII

LEGAL ISSUES IN CYBER ADVERTISING

Advertising is an important industry in the Meta society as well as the Internet society. The Internet Advertising industry is a US $ 7.2 billion (Rs 3600 crore) per annum industry growing at a rate of around 15 to 20 % annually.

Advertising being basically a "Communication" and Internet, basically a "Communication Medium", there is a synergy between the Advertising industry and the Internet.

Simultaneously, there are innumerable number of legal issues arising out of Cyber Advertising.

In order to fully appreciate the legal issues involved in Cyber Advertising, let us first try to understand the background of Cyber Advertising and some of the technology aspects that go with it.

ESSENCE OF ADVERTISING

Advertising is a key ingredient of Marketing in any business strategy. It's relevance has increased with global market economy replacing regionalized protected marketing in the business world.

Essentially, Advertising is a "Message" from the producer of a product or a service to a "Potential Consumer", aimed at motivating "Purchase". It can be released through the Press as a print media communication or through the radio as an Audio message or through the TV as a multi media message with audio and Video.

Advertising can serve all other principles of marketing such as,

- ❖ Awareness Creation
- ❖ Interest Creation
- ❖ Desire Creation
- ❖ Availability Information Dissemination and
- ❖ Satisfaction enhancement of the customer.

In order to achieve the desired objectives, messages are suitably structured and exposed to the target audience, keeping in mind the psychological impact that a message can create in a given environmental background and individual's frame of mind.

The distribution and the sales process complement the advertising process to fulfill the marketing objectives.

THE CONCEPT OF THE MEDIA

The vehicle that transmits the advertising message to the audience is the "Media". Print, Radio, Television, Outdoor Display are different kinds of media that have been prevailing from a long time for mass communication of an advertising message.

Direct mailers have been used for more targeted advertising message delivery. Additionally several innovative media have been used to reach out to specific audiences with greater emphasis. Today, a Cricketer's shirt and the bat is also an advertising space considered valuable.

INTERNET AS A MEDIA

The advent of Internet has introduced a whole new concept in advertising since Internet was a media which actually combined

the best characteristics of the Print, Radio, TV and Direct Marketing media.

Internet as a media is a "Multi Media" vehicle which can carry text, audio and video messages to the target audience. In this respect, it is like a TV medium.

Internet can carry through hyperlinks, details that a TV ad cannot carry but a print ad can. Even a Statutory Prospectus ad of an IPO (Initial Public Offer or Public Issue) can be effectively displayed on the Internet but not in the Radio or TV.

Unlike a TV which is an invasive media, Internet is a non invasive media and the consumer on his own accord visits various locations on the Internet which may carry advertising messages. Internet is an "Interactive Media" where the ad information is mostly pulled out on request by the consumer.

Internet can also don the "Invasive media" role when it uses the "Push Technology" and E-mail for advertising. The pop up ads also are in a way intrusive in nature.

Internet provides the possibilities of "Micro Packaging" of a product and "Mass Customization" of both the product and the advertising message.

While a detailed analysis of the merits of Internet as an advertising media is not within the scope of this book, it is essential to appreciate that Internet is in many ways an ideal media for advertising. If properly used, it can be both customer friendly and effective.

RELEVANCE OF ADVERTISING FOR CYBER COMMUNITY

Internet is historically a media which recorded the fastest growth in terms of reach. If we take a reach of 5 million as a bench mark, it is said that the Radio took 30 years to reach this level while the TV took 14 years. On the other hand Internet is supposed to have taken just 5 years to reach this mile stone.

Availability of high value content, mostly free of cost to the consumer was one of the most important factors that contributed to the quick adoption of Internet as a media and also enabled E-Commerce to develop.

The availability of this "Free Content" itself can be attributed to the financial support that was promised to the content owners through "Advertisements".

During the hey days of dot com economy, "Eye Balls" were valued for their advertisement potential which reflected in the corporate valuation. Services were offered free in exchange of "Page views". Software were given free in exchange of advertising exposure it generated. ISP s gave the connectivity free and traded it for advertising.

One of the reasons for the failure of the so called "Dot Com Economy" subsequently, was the decline in the advertising potential over the Internet partially due to the Cyber Law regime itself stifling the growth of Cyber Advertising.

Hence the future of Cyber Advertising is also irretrievably linked to the impact of Cyber Laws on many of the aspects of Cyber Advertising as we shall briefly discuss in this chapter.

It is in the interest of all Cyber Advertising professionals and Internet Economy observers to ensure that Cyber Laws do not become too rigorous and kill advertising opportunities because it is the "Advertising" that can bring down the cost of Internet usage.

TYPES OF ADVERTISING ON INTERNET

Internet is a vast agglomeration of technology which has many facets such as the Web, E-mail, Discussion Board, E-mail list etc.

Accordingly there are also many ways in which advertisements can be used on the Internet.

WEBSITE AS AN ADVERTISEMENT

Initially when the World wide web was new to the Meta society corporate world, "Website" itself was a means of Cyber Advertising. Companies used the website as a "Corporate Brochure on the Net" so that the international audience could get the first information on the company through the Internet.

With the passage of time, the web site has evolved from being a mere corporate brochure to a " Communication Interface with the stake holders of a Corporate entity". It is also the main transaction space for many businesses.

Even though the website still performs the role of providing corporate information to the public and therefore still has an "Advertising Character", calling website an "Advertisement" would be a gross undervaluation of the potential of the website. It is like calling the "Visiting Card" or the "Corporate Headquarters" of a company, an advertisement.

Even then, this obsolete concept of considering website as an "Advertisement" finds a mention in the Indian regulations through the Advertising guidelines issued by IRDA (Insurance Regulatory and Development Authority) which lists the website of an insurance company as an "Advertisement" and subjects it to some regulations.

BANNER ADVERTISING

By far the most important type of Internet advertising is the "Banner Advertising". Banner advertising appears as a piece of distinctive text or image embedded into the contents of a web page with a short message. It is then hyperlinked to the web page containing more details about the advertiser or his message.

The banner may appear on the top of the page or any other space which the page designer thinks is appropriate. It comes in different sizes also.

Multi Media Banners

The advertising banner can be a static image containing the message or an animated image. If the bandwidths permit, the banner can be multi media banners also.

Dynamic Selection of Banners

One of the special characteristics of the Internet as an advertising media is that the banners to be displayed on a given space can be managed in such a manner that its effectiveness as a messaging tool can be enhanced through various technical means.

For example, the banners can be served on rotation basis from a pool of pre selected banners rotated on a variety of decision parameters.

The objective of ad rotation could be that if the same person is visiting a web page a number of times he need not see the same ad. The same advertiser can release different messages which may be progressively motivating messages for the sale of a product or different messages for sale of different products.

Some times the number of exposures that a given page can provide is too large for a single advertiser and there is a cost benefit if the ad space can be shared by different advertisers. In such a case the ad rotation has to be done by some body who aggregates ad space utilization for different advertisers.

The banner ad rotation is also useful for displaying "Targeted" ads based on the type of visitor to the web page. For example, a visitor from India to Sify.com may be exposed an advertisement of a Car Loan from ICICI Bank while a visitor to the same page from USA may be exposed with an advertisement of Mortgage Loan from an American Bank. Such targeting is possible on various parameters such as the likely place from which the person is visiting, the time of the day, the previous web page from which he came in etc.

To achieve such a banner ad rotation, the filler for the banner ad space is allotted an identification "Tag" by the web page designer. The "Tag" is then linked to a data base element consisting of the different ad materials from which a selected piece is displayed. Normally the link between the "Tag" and the advertising material is managed by the website owner or a specialized a "Ad Serving Agent".

There are several legal consequences arising out of the "Ad Rotation System" which will be discussed in detail subsequently.

Refreshed Banner Ads

Normally the Banners are rotated when a person enters the page and then the banner remains until the visitor leaves the page. In case a web page is one which the user is likely to keep open for a long time, then the banner may be refreshed from time to time even while the visitor remains on site. Such ads are like the TV commercials which keep coming one after the other in the same channel.

POP UP ADS

Yet another way of displaying ads is through a separate window which either pops up when a visitor enters a page or leaves a page or clicks on any item on the page etc. Such pop up ads may occupy the entire window or a smaller portion and also programmed to reappear when an attempt is made to close them.

ADS IN E-MAILS

The e-mail software used at present such as the Outlook express and Netscape Messenger, are equipped to display not only text messages but also html pages. It is therefore possible to treat each e-mail as a "web page" and incorporate all the banner advertising principles in the html format of the e-mail.

E-Mail news letters are normally designed just like a web page with ad space being allocated at various places in the mail.

E-Mail itself can be considered as a "Direct Mail Ad" as it is targeted to a specified individual. Here again customization of the highest order is possible for the advertisement messages.

SEARCH ENGINE ADS

Yet another type of ads are those used by search engines. Search engines display the search results of their users in a separate page with hyper links to the respective search results and a brief description of the content. Normally the search results are listed in the order of their relevance to the search query with the most appropriate search result appearing on the top.

There are two special advertising options that search engines normally provide. One is the "Key Word linked" banner ad display. Second is the "Top Listing" on payment basis where the advertiser's web site is displayed as a part of the search result at the very top.

There are special legal issues that arise out of such advertising which are discussed later.

ADVERTISING MEASUREMENT

One of the important aspects of Advertising which is relevant to the advertiser and the publisher is the measurement of the effectiveness of advertising. The usual manner in which a print ad or a TV ad is measured is in terms of "Potential Exposure" based on the available circulation or viewer ship statistics.

On the Internet , the measurement is more accurate since the exposure is directly linked to the number of visitors who arrive at particular space where the ad is displayed.

In the case of a "Banner Advertisement", the first parameter to verify the effectiveness of advertising is to measure the number of "Page Views". i.e., the number of times the web page is viewed. Such views can be by the same person or different persons. If a banner is constantly exposed on a web page, the number of page views can be equivalent to the number of "Ad Views".

However, since most of the time, the visitor may pass trough the page without spending enough time on the page for letting the banner file down load, the actual "Ad Views" will always be less than the page views.

Some of the users also use various techniques and software to block banner advertisements to speed up surfing. The Ad-views may also be reduced for this reason.

In case the banner ad space is shared, then the actual ad views will have no relation to the page views. The actual measurement in this case has to be done by the "Ad Serving" software at the time the ads are served on rotation. Even here there will be loss of exposure due to the visitor moving out of the page quickly or using an ad blocking technique.

Despite these short comings, the Banner Ad method of advertising is the most commonly used strategy for web advertising.

PAYMENT METHODS

Advertising payments on the web are often linked to the number of exposures of a given ad. For example a rate of Rs 750 per mille means that the cost of advertising is Rs 750 for 1000 exposures.

In case of small web sites and sponsored web pages the rates may be quoted on the basis of "Per unit of period" such as "Per Month".

In certain cases the advertising payment is also linked to "Number of Click throughs" instead of "Number of Exposures". Here the payment is based on the exact number of clicks achieved by the Banner.

LEGAL ISSUES

General Laws of Advertising fall under the law of contracts. Basically, Advertising is a contract between the "Advertiser" and the "Publisher" where a certain message of the advertiser is inserted within the publication.

The advertisement message belongs to the advertiser and there is no endorsement of the same by the publication. This is in direct contrast to the "Editorial Content" in the publication for which the publication has a responsibility.

The advertisement is, on the other hand, a third party message on which it does not have full control.

In the print media, the advertisement material is physically handed over to the publisher before the final printing. It is therefore technically possible for the publisher to reject an advertisement if he deems it fit to do so.
All print publications therefore support certain "Basic Ethics of Advertising" which incorporates the principles of "Being Fair and Truthful" in communication.

"Misrepresentation" and "Fraud" are the two contractual risks that the advertiser and the publisher have to encounter. Any advertisement which is prima-facie untruthful and designed to mislead a consumer, may be held to be a "Fraud". On the other hand "Exaggeration" is a basic nature of advertisement and it often leads to "misrepresentation".

Advertising of specific services such as Health and Financial Products, as well as advertisements aimed at Children may come under special laws in some countries.

ICC GUIDELINES ON WEB ADVERTISING

The International Chamber of Commerce (ICC) has issued some guidelines in respect of Internet Advertising. The guidelines are meant to enhance the confidence of the public at large on the Advertising and safeguard the consumer interests. At the same time it is also to safeguard the freedom of expression for the advertisers and to minimize the need for Government regulations.

The salient features of the guidelines are:

1. Legality:

All advertising and marketing should be legal, decent, honest and truthful. "Legal", in the context of these guidelines, is presumed to mean that advertising and marketing messages should be legal in their country of origin.

2. Social Responsibility:

Advertising and marketing messages should be sensitive to issues of social responsibility and should in addition conform to generally accepted principles as regards ethical marketing.

3.Confidence Building:

Advertising and marketing messages should not be designed or transmitted in such a way as to impair overall public confidence in the Internet as a medium and marketplace.

4. Identity Disclosure :

Advertisers and marketers of goods and services who post commercial messages via the Internet should always disclose their own identity and that of the relevant subsidiary, if applicable, in such a way that the user can contact the advertiser or marketer without difficulty.

5. Cost Disclosure:

Advertisers and marketers should clearly inform users of the cost of accessing a message or a service where the cost is higher than the basic telecommunications rate. Users should be provided with such notice of cost at the time they are about to access the message or service. This notice mechanism should allow users a reasonable amount of time, as set by the marketer or mandated by applicable law, to disconnect from the service without incurring the charge.

6. Advertising in News Groups:

Advertisers and Marketers should respect the role of particular electronic news groups, forums or bulletin boards as public

meeting places which may have rules and standards as to acceptable commercial behaviour.

Advertising and Marketing messages posted to public sites are considered appropriate:

- when the forum or site receiving the message has a fundamentally commercial nature or activity; or
- when the subject or theme of the bulletin board or news group is pertinent to the content of the advertising or marketing message; or

when the forum or site has otherwise implicitly or explicitly indicated consent to the display.

7. Collection and use of data

Advertisers and marketers should disclose the purpose(s) for collecting and using personal data to users and should not use the data in a way incompatible with those purposes. Data files should be accurate, complete and kept up to date.

8. Data privacy

Advertisers and marketers should take reasonable precautions to safeguard the security of their data files.

9. Disclosure of data

The user should be given the opportunity to refuse the transfer of data to another advertiser or marketer. Personal data should not be disclosed when the user has objected except by authority of law. Online mechanisms should be put in place to allow users to exercise their right to opt-out by electronic means.

10. Correction and blocking of data

Advertisers and marketers should give the user the right to obtain data relating to him and, where appropriate, to have such data corrected, completed, or blocked.

11. Privacy policy statements

Advertisers and marketers are encouraged to post their privacy policy statement on their online site. When such privacy policy statements exist, they should be easy to find, easy to use and comprehensible.

12. Unsolicited commercial messages

Advertisers and marketers should not send unsolicited commercial messages online to users who have indicated that they do not wish to receive such messages. Advertisers and marketers should make an online mechanism available to users by which the users can make known to the advertisers and marketers that they do not wish to receive future online solicitations. Unsolicited online advertising or marketing commercial messages should be clearly identified as such and should identify the advertiser or marketer.

13. Advertising to children

Advertisers and marketers offering goods or services to children online should:

- not exploit the natural credulity of children or the lack of experience of young people and should not strain their sense of loyalty;

- not contain any content which might result in harm to children;
- identify material intended only for adults;
- encourage parents and/or guardians to participate in and/or supervise their children's online activities;
- encourage young children to obtain their parent's and/or guardian's permission before the children provide information online, and make reasonable efforts to ensure that parental consent is given;
- provide information to parents and/or guardians about ways to protect their children's privacy online.

14: Respect for the potential sensitivities of a global audience

Given the global reach of electronic networks, and the variety and diversity of possible recipients of electronic messages, advertisers and marketers should be especially sensitive regarding the possibility that a particular message might be perceived as pornographic, violent, racist or sexist.

Applicability of ICC Guidelines

The ICC Codes and Guidelines are always subordinate to existing national law. In the Internet scenario, there is always a debate on whether the laws of the Country of the consumer or the laws of the advertiser is applicable.

Normally jurisdiction in a contract is determined by the terms of the contract itself. In the same way, a web site may display through a notice or through the terms and conditions that the laws of one place or the other is applicable for the transactions.

This has however been challenged by at least the South African E-Commerce legislation which has provided protection for its citizens entering into E-Commerce, based on specific provisions in the Electronic Communications and Transactions Act 2002.

The proximity of the place of business to the consumer is another criteria used in US to resolve interstate jurisdiction. Accordingly, if a Company has a branch in California, its dealings with the citizens of the Californian state will be determined by the local laws even if the head office of the company is elsewhere.

In India, while there are no laws passed for Internet advertising or Netizen Consumer protection, the provisions of ITA-2000 will apply to determine the jurisdiction of contracts. Accordingly, the place of residence of an individual and the place where the head office of a company is located are considered the relevant points where the offer and the acceptance take place.

The place where the server is located or the place from which the actual access was made by the consumer is not relevant in determining the jurisdiction. Additionally, since the Indian Advertising industry has its own norms for the Print and Electronic media through the Advertising Standards Council, the same may be extended to all advertisers operating within the jurisdiction of India.

HEALTH RELATED CYBER ADVERTISING

The provisions of HIPAA has been discussed in detail in the chapter on "Privacy". In as much as data of a consumer in the hands of an advertiser is concerned, the privacy protection aspects of HIPAA becomes applicable if the organization is otherwise covered under the Act.

FINANCE RELATED CYBER ADVERTISING

The guidelines of the Security Exchange Board of India will apply to the Companies and financial intermediaries in respect of any advertising and financial communication in the web. Similarly in USA, the guidelines of the Security Exchange Commission and the provisions of the GLBA (Discussed in detail under privacy laws) are considered applicable to the entities covered by their guidelines.

INSURANCE RELATED ADVERTISEMENT IN INDIA

The Insurance Regulatory and Development Authority of India, (IRDA) which is the apex regulatory agency in India has listed both Website and E-Mail as "Advertisements" for the purpose of their advertisement guidelines.

Apart from the provisions of being truthful etc, this provision means that the "Advertising Compliancy Officer" who has to be mandatorily appointed under the IRDA by the Insurance Companies, has the responsibility of monitoring the contents of the web site and e-mails and ensuring that they fall within the guidelines.

Considering the detailed requirements that the IRDA guidelines have prescribed for Insurance advertising, it is evident that it is practically impossible for ensuring that the guidelines are fully followed in respect of the website and the e-mail.

However, until IRDA removes this in advertent listing of websites and e-mails as "Advertisements" per-se, there is a Damocles sword hanging on every Insurance company operating in India and using Internet for its communication.

RBI GUIDELINES FOR WEBSITES OF BANKS

The Reserve Bank of India (RBI) has issued guidelines to banks conducting transactions on the Internet.

According to one of the guidelines regarding use of "Hyperlinks", the guideline states

> "Hyperlinks from Bank websites often raise the issue of reputational risk. Such links Should not mislead the customers into believing that they sponsor any particular product or any business unrelated to Banking. Hence hyperlinks from bank's sites should be confined to only those portals with which they have payment arrangement or sites of their subsidiaries or principals."

A strict reading of this guideline indicates that banks are prohibited from carrying any advertisements on their sites other than of their own or their subsidiaries or principals.

THE ROLE OF AD SERVERS

The popular method of serving ads through third party "Ad Servers" introduces an intermediary in the process of advertising which is otherwise a contract between the advertiser (through the advertising agency in some cases) and the publisher.

The Ad server normally acts as an agent of either the advertiser or the publisher and it is essential for the principal to disclose his existence to the other party to the contract in order to determine the inter-se liabilities.

In some cases the publisher would have engaged the services of the Ad server to market its ad inventory and to provide value added services such as ad-rotation, statistics collection etc. In that case the ad material given by the advertiser to the publisher may actually be hosted in the server belonging to the Ad Serving company. There may be "Conflict" issues such as the Ad Serving Company dealing with competing clients and using the same ad space alternatively between different competing advertisers.

Imagine the top banner in sify.com alternately showing a Pepsi Ad and a Thums Up counter Ad. Neither of the advertisers would be happy with such an arrangement which they might have actually banned by contract with their advertising agencies.

Apart from the legal consequences, there are also issues of "Ethics" in advertising business which would affect such indirect relation between the advertiser and the Ad Server.

The storing of the ads in a server different from that of the publisher may also lead to damage or misuse occurring through hacking or virus attacks on the server of the Ad Serving Company. This is another grey area which could create legal problems if the contract does not specify the inter-se liabilities in such cases.

Imagine the consequences of a hacker replacing the Pepsi messages into Coca Cola messages and the ads getting released at the expense of Pepsi. Unlike a print media where a "Voucher Copy" of the publication can be obtained for each ad, there is no way millions of exposures are tracked by either the advertiser or the publisher.
The involvement of the third party ad server has to be therefore properly disclosed by their principals and the responsibilities clarified at the time of entering into advertising contracts.

THE ROLE OF MARKETING AGENCIES

One of the essential features of advertising is to collect information about the advertising value of a publication such as the number of visitors (Traffic), the profile of the visitors (Demographics as well as psychographics). The web technology provides the facilities to track not only the number of visitors, but many of his browsing habits including how long he stays on the page, where from he comes and where to he goes etc.

While the visitor may not be personally identified, he can be tracked with reference to a cookie planted in his computer.

If however, the visitor is a member of any other data base on the Internet where he has provided his personal data, the cookie may tag the identifiable Meta society data with the Cyber space activity of the person seriously compromising his privacy.

TRACKING PROGRAMME AND COMPUTER CONTAMINANT

Some of the advertising aggregators who have a larger stake in following the browsing habits of the Netizens plant programmes with or without disclosing their full functionality, in the computers of the Netizens. Such programmes can be misused to draw private information of the user.

If planting of such programmes are not properly disclosed, and consent obtained from the user, they may be classified as "Computer Contaminants" under Section 43 of the ITA-2000 and the person responsible for such planting, may be called upon to pay compensation up to RS 1 crore to the affected person.

PROTECTION FROM LEGAL CONSEQUENCES

It is evident that the legal implication of Cyber advertising can be tricky. The technical possibilities and the marketing requirements often provide enough incentives for the marketing personnel to transgress the limits of legal provisions by design or ignorance or convenient interpretation.

Corporate mangers who manage business risks should however ensure that the legal risks are properly covered by adequate disclosures on the web sites placed in close proximity to the advertisement and also through proper contractual back ups.

Today, the advertising guidelines issued by ICC are observed more in the breach than in compliance. However, as the Cyber Law awareness in the community grows, the risks of non compliance could lead to disastrous consequences for the advertiser and the publisher. They should therefore develop a suitable Cyber Law Compliancy policy to protect their interests.

CHAPTER XIX

LEGAL ISSUES IN CYBER BANKING

Banking was one of the earliest industries in the world to have adopted Internet into its Business Model. Initially, the dot-com banks made significant progress in USA and elsewhere in the world just as Amazon.com made its presence felt as a virtual book seller. Gradually the Brick and Mortar Banks joined the race and today they use Internet as a means of communication not only for Customer transactions but also for Inter-branch transactions and Inter-bank transactions.

In India, the strict licensing regime in the Banking industry has ensured that no Virtual bank could come up on the Net. However, the Commercial Banks entered the Cyber space initially with an information website and later with limited online transactions. Today, without doubt ICICI Bank is the leading Indian Bank on the Net with HDFC Bank, UTI Bank, SBI and others trying to catch up with them.

The Competitive environment in which Commercial bankers have to function today in India has also placed a premium on

- Reduction in Cost of Service
- Innovation in Products
- Better Customer Service.

Technology Banking in the Internet era will therefore try to achieve these objectives by the use of Internet.

The legal issues confronting the Cyber Banks of India have to be analyzed with reference to the general legal regime prevailing in

India and the specific guidelines that have now been issued by Reserve bank of India in this regard.

BUILDING BLOCKS OF TECHNOLOGY BANKING

Technology Banking in the Internet era will be characterized by

1. Establishing customer relationship on the Internet and maintaining them through Internet for a true "Any where, Any Time" Banking service.
2. Interacting with the existing clients through Internet for communication.
3. Using Internet for structuring and delivering services that require automatic real time responses such as the Foreign Exchange and Treasury Operations besides the Stock Market Payment mechanisms.
4. Inter Bank Fund Transfer and Clearing of cheques through Internet.

LEGAL ISSUES

Digital Signatures:

The Banker Customer relationship in the Internet era will revolve around the Digital signatures as it now revolves round written signatures. In view of the Digital Signature being a creation of Technology, The Banker would be heavily dependent on technology for "Authentication", "Storage" and "Recovery" of information.

Customer Relation Establishment:
In the Meta society Banking, opening of accounts are always done with the Customer and the Introducer being present before an authorized Bank officer. With the passage of the Information Technology Act, a natural question that will come up is whether an Account can be opened through Electronic Documents only**.**

For records sake, the RBI guidelines on Internet Banking released on June 14, 2001 has indicated that Banks should open accounts only after physical verification of signatures. This implies that the guideline is over ruling the spirit of Section 4 and 5 of the Information Technology Act 2000 according to which an electronic application made with a digital signature covered by the Digital Certificate from an approved Certifying authority should be a legally valid application for starting a Banker-Customer Contractual relationship. .

The action can be legally justified only by extending the provisions of Section 9 of the ITA-2000 to RBI . However Section 9 was meant to provide a discretion to the Government and some of the Government agencies not to adopt E-Governance measures enunciated in sections 6, 7 and 8. It is doubtful if the legislative intent was to exempt RBI from these provisions.

Presently, RBI is has become a Certifying Authority itself through its technology arm IDRBT (Institute of Development and Research in Banking Technology). RBI also has initiated amendments to Negotiable Instruments Act 1881 and the ITA-2000 itself to provide recognition to electronic form of cheques. It is time therefore for RBI to review its Internet Banking guideline and withdraw the ban on opening new accounts through digitally signed application forms.

Rights of Lien and Setoff:

Banking law and practice have developed some exclusive laws applicable to Bankers particularly in the areas of Lien and Set off. While "Lien" refers to physical property, "Set off" refers to moneys due.

In the Internet banking era, the "Virtual Properties" and "Virtual Balances" come to the forefront. The established Banking law and practice will have to therefore modify itself to accept lien of a virtual property and set off on virtual money.

Negotiable Instruments and the ITA-2000:

Law and Practice of Indian Banking have been developed on the basis of English law and are fairly well established. The Negotiable Instruments such as the Cheque, Bill of Exchange and the Promissory Note have a legal history of their own. With the advent of Internet into Banking, many of these need to undergo a change.

When Information Technology Act-2000 was originally passed, it stated in its first section itself that the Act shall not apply to a Negotiable Instruments. Now this restriction has been confined to Negotiable Instruments other than a Cheque meaning the Promissory Note and the Bill of Exchange.

The Negotiable Instruments Amendment Act 2002 (NIAA-2002) has introduced two types of Electronic Instruments called the Electronic Cheque and the Truncated Cheque and ITA-2000 would be applicable for such cheques.

Promissory Notes and Bills of Exchange are however outside the scope of the ITA-2000.

The Electronic Cheque has been defined under NIAA 2002 as under:

> "a cheque in the electronic form" means a cheque which contains the exact mirror image of a paper cheque, and is generated, written and signed in a secure system ensuring the minimum safety standards with the use of digital signature (with or without biometrics signature) and asymmetric cryptosystem;

Similarly, the truncated cheque has been defined as under:

> "a truncated cheque" means a cheque which is truncated during the course of a clearing cycle, either by the clearing house or by the bank whether paying or receiving payment, immediately on generation of an electronic image for transmission, substituting the further physical movement of the cheque in writing.

RBI is presently working on the procedures involved in operating the truncated cheque and e-cheques. It is however clear that the truncated cheque being a system internal to the Banking system, it is possible to install necessary equipments and truncate the physical cheques. However, the concept of Electronic cheques to be used by the public is more difficult to implement since it requires a hardware device for the purpose of converting a physical cheque to a cheque in Electronic form.

Even though this is an attempt to introduce an electronic cheque in the Indian system, the suggested system is incomplete without appropriate systems for endorsement and delivery of E-Cheques.

In the meantime, if a Customer issues a digitally signed instruction to his Banker containing all the ingredients of a cheque such as an unconditional order to pay a certain sum of money to a certain person, it is legally inconceivable not to recognize the nature of this instruction as an E-Cheque.

While the Banker is at liberty to bar such instructions by specific contract, if the Banker Customer Relationship is based on a contract, which is silent on this aspect, the instruction cannot be ignored. If the instruction is refused and consequently the beneficiary is forced to a financial loss or damage, which in turn results in a loss to the customer, the Bank may have to compensate.

It may be recalled that even in Meta society Banking, a letter written by a customer ordering the bank to make a certain amount of money to a certain person to the debit of the customer's account is always honoured.

Even though Clearing houses do accept some letter like instruments such as IT refund orders, and Traveller's cheques, customer's letters are not an accepted instrument for clearing purpose. But for this short coming, the letter is still binding on the Banker to whom it is issued. Hence a similar electronic instruction cannot be ignored by the Bankers.

DIGITAL SIGNATURE CANNOT TALLY WITH A SPECIMEN

When it comes to "Signature", Banks adopt a "Procedure" where by the signature should be as per the specimen already supplied to the Bank.

One important aspect of Digital Signature is that it is irretrievably linked to the document and no two digital signatures ever tally. It will require a totally different out look for the Bankers to accept a payment instruction where the "Digital Signature is not tallied with any specimen already supplied by the customer.

Further, the Digital Signature even though may be as safe as the written signature, relies on a Certifying authority for authentication. It would therefore make the Banker subordinate to the Certifying Authority as regards authenticating a signature.

Termination of Banker Customer Relationship:

Bankers may receive e-mails notifying "Death", "Insolvency" or "Insanity" of the customer which, like the stop payment instructions would put them in a dilemma.

The dilemma is basically on the need to identify and authenticate the message. As in the usual case of such information being received over phone or through third party unconfirmed sources, the Bank Manager has to use his discretion in acting on such messages.

E-Mail Identifiers for Bank Staff:

In the context of receiving notices that affect banker-Customer relations, it becomes relevant to discuss the effect of e-mail addresses such as manager@xyzbank.com or ashok@Indianbank.com. If a third party is sending a mail at manager@xyz.com, it may be considered a valid notice to the Bank while the personal name at the bank's address may be considered as a personal message. Banks will have to carefully develop their policies of providing e-mail identities to their authorized staff.

Banking in a Continuous Time Cycle:

Another important aspect of Banking in the Internet era would be that one single Internet Interface center would be able to cater to customers in different time zones. Hence the Internet Bank is a 24-hour Bank. The Bank has to therefore consciously introduce a

day change over so as to give effect to policy changes. Unlike in Meta Society Banking where the Banker and Customer are in the same time zone, in the Internet Banking zone, if the rate of interest is to be changed, one has to be specific that the change is effective with effect from X hours IST.

Every Banking transaction has to be therefore time stamped and the time becomes an important parameter of the voucher.

Security in Banking Environment:

So far when we spoke of security in the Banking environment, we spoke of "Physical Security". In the Internet era, Security has to be seen not only at the Physical level, but also at the "Data Storage Level". Apart from having a security guard at the door, it will therefore be necessary to have a "Fire Wall" protecting the data.

Just as we distribute "Key" s to the safe at present, the Banking in the Internet era would consist of "Passwords" as keys or "Smart Cards" as Key holders.

Hacking and Virus will be the tools of fraud more than "Forgery" and "Dacoity". The Banker in the coming era should prepare himself to deal with these technological threats to remain in business.

A detailed guideline on security has been issued by RBI which has been separately reproduced at the end of this chapter. It is interesting to note that the guidelines suggests the Banks to use the services of "Ethical Hackers" to monitor the security levels of the network.

Real Time Information Products:

Another feature of Internet is its ability to collate information from many sources on a real-time basis. This aspect of Internet would come in handy for Bankers in structuring products in areas such as "Foreign Exchange" or "Treasury ". For example, every foreign exchange bid can be reverse auctioned on the Internet for obtaining best market rates directly from the customers with counter offers. The Banker in this case will only act as a trusted intermediary to enforce the contracts.

Once the exchange control regulations remove the concept of an "Authorized Dealer" and permit direct customer level contacts, a normal E-Commerce portal such as paisepower.com can substitute the Bank in brokering foreign exchange transactions. Bankers have to be on their toes as otherwise the prediction of Mr A.T. Pannerselvam, former IBA chairman that "Future of Indian Banking will belong to Non Bankers" will come true.

Virtual Property As Security:

Bankers will increasingly come across requests to evaluate and accept Properties such as web sites as security for loans. At present Banks conveniently avoid such decisions by refusing the security and insisting on "Land and Building". However, in the coming days, wealth will concentrate with people who accumulate Intellectual Property and Virtual Property and business from such customers will shift to those progressive bankers who are capable of accepting these properties as security.

AMENDMENTS TO BANKER'S BOOKS EVIDENCE ACT AND RBI ACT

Realizing the growing importance of electronic documentation in Banking, the ITA-2000, has proposed some vital amendments to

the Bankers Books Evidence Act 1891 as well as the RBI Act 1934

According to Schedule 3 (Ref: Sec 93) of the ITA-2000,

Banks can now store "Ledgers", "Day Books", "Cash Books", "Account Books" etc in the form of floppy, Disk, Tape or other electromagnetic data storage devices.

"Certified Copy" of transactions include print outs of data stored in a floppy, disc, tape or any other electromagnetic data storage device together with a statement certified as under:

-**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

-**a certificate** by a person in-charge of computer system containing a brief description of the computer system and the particulars of - .

the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons

the safeguards adopted to prevent and detect unauthorized change of data;

the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices

the mode of verification in order ensure that data has

been accurately transferred to such removable media;

the mode of identification of such data storage devices the arrangements for the storage and custody of such storage devices;

the safeguards to prevent and detect any tampering with the system; and

any other factor which will vouch for the integrity and accuracy of the system.

- a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief that the 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 amendment to the RBI Act as per Schedule 4(Ref Section 94) empowers RBI to extend its powers regarding regulation of Fund Transfers between Banks to "Electronic Means of Fund Transfers" also. Cama Committee on E-Money.In one of the recent attempts to exercise its control on E-Commerce, a working group constituted by RBI on E-Money has come up with suggestions on electronic systems that can be used as multi-purpose e-money.

The Working group headed by Mr Zarir J Cama which submitted its report on July 11, 2002 has expressed its opinion that the Electronic Payment Systems have the potential to become an independent medium of exchange and therefore needs to be regulated.

Accordingly the group has recommended that

-e-money for multipurpose use can be issued only when the payment has been made by the e-money holder in full through Central Bank Money.

-Issue of e-money against credit is recommended to be restricted to Banks.

-Only single purpose e-money is recommended for use by other entities.

It also suggests that where e-money is issued in exchange of any other kind of services, a "Redemption Option" should be provided for conversion into Central Bank Money.

These recommendations may shortly be codified into appropriate legislations. There will however be many more areas of operation in Banking where the traditional legal interpretations will have to be redefined to suit the requirements of Technology Banking in the Internet Era.

Internet Banking in India – Guidelines
(June 14, 2001)

Reserve Bank of India had set up a 'Working Group on Internet Banking' to examine different aspects of Internet Banking (I-banking). The Group had focused on three major areas of I-banking, i.e.,

(1) technology and security issues,
(2) legal issues and
(3) regulatory and supervisory issues.

RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly, the following guidelines are issued for implementation by banks.

Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues.

I. Technology and Security Standards:

a. Banks should designate a network and database administrator with clearly defined roles as indicated in the Group's report.
b. Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.

c. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.
d. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.
e. All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.
f. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:
    1. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.
    2. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like

passwords in transit within the enterprise itself.

g. It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server.

h. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.

i. The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:
    1. Attempting to guess passwords using password-cracking tools.
    2. Search for back door traps in the programs.
    3. Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
    4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.

5. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').

j. Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

k. Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically.

l. All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.

m. Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

II. Legal Issues

a. Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer.

Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer.

b. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.
c. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks.
d. In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.
e. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and

liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks.

III. Regulatory and Supervisory Issues:

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1. Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.
2. The products should be restricted to account holders only and should not be offered in other jurisdictions.
3. The services should only include local currency products.
4. The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-

border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.

5. Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor.

Given the regulatory approach as above, banks are advised to follow the following instructions:

a. All banks, who propose to offer transactional services on the Internet should obtain prior approval from RBI. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them.
b. Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks.

c. The guidelines issued by RBI on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks.
d. Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misutilizing the same, etc., effectively.
e. With the increasing popularity of e-commerce, it has become necessary to set up 'Inter-bank Payment Gateways' for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted.
f. Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway.)

g. Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time.
h. Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway's end and the participating institutions' end certified prior to making the facility available for customers use.
i. Bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law.
j. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net.
k. Hyperlinks from banks' websites, often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business

unrelated to banking. Hyperlinks from a banks' websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers' purchases.

2. The Reserve Bank of India have decided that the Group's recommendations as detailed in this circulars should be adopted by all banks offering Internet banking services, with immediate effect. Even though the recommendations have been made in the context of Internet banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant.

3. All banks offering Internet banking are advised to make a review of their systems in the light of this circular and report to Reserve Bank the types of services offered, extent of their compliance with the recommendations, deviations and their proposal indicating a time frame for compliance. The first such report must reach us within one month from the date of this circular. Banks not offering any kind of I-banking may submit a 'nil' report.

4. Banks who are already offering any kind of transactional service are advised to report, in addition to those mentioned in paragraph above, their business models with projections of cost / benefits etc. and seek our post-facto approval.

CHAPTER XX

LEGAL ISSUES IN EMERGING TECHNOLOGIES

When the web started, the language of the web was the "HTML". The web content was held in the web server as a "HTML File" and recalled by the Netizens through the URL typed on the browser window or through an automated process of clicking on the hyper links from other web pages. Such "Hyper Linking" itself gave raise to many legal disputes such as "Framing" and "Deep Linking" which are not yet fully resolved even today.

However, the identification of an electronic document which might have been subject to dispute was at least possible with a given URL and this clarified many of the requirements of law.

XML AND SCRIPTS

In the mean time several new developments are complicating the legal issues of Web Content Creation and Delivery. For example the XML language that is replacing the HTML for creation of web pages through custom built tags is emerging as a standard for some aspects of Electronic Document creation replacing the HTML.

Similarly, the embedded scripts either at the client level or at the server level or Applets determine what content is seen by the user and in what design and form. The existence and identification of the Electronic form in a particular form is therefore relative to many aspects some of which are configurations that the user sets

up voluntarily .

For example, if there is a well highlighted "Disclaimer" on a web site in the form of a image and the user has turned off the "Image Viewing Facility" in his browser or his "Ad Removal Software" wrongly blocks the image, there would be a dispute on who is accountable for the actions that result out of the user not getting the "Disclaimer Message".

Is it the user who has configured his machine not to view the images or is it the web site owner who has put the disclaimer in a form that is known to be blocked by a software. This may also be determined on the basis of whether the software in question is in limited or wide spread use.

DYNAMIC CONTENT

The emergence of Dynamic Content Creation through a process of "Creating a Web Page on the fly" by aggregating different components put together by a decision rule triggered by the identification of the customer or his browser, or his location or the time of the day etc creates unique legal challenges.

For example, let us say that there is a site that displays obscene material if you use a customized browser (Or a Special Browser Plug-in) distributed by the site owner or his associate but displays harmless pages when you use an Internet Explorer or Netscape. Should law consider this as "Distribution of Obscene Material in electronic Form tending 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." as defined by Section 67 of the ITA-2000?

Further, if an electronic document is custom built for a single

person based on his known or perceived preferences, then in case of a dispute, it would be extremely difficult for the person to produce evidence in a court in an acceptable manner. The disputed document may not be easily reproducible at another point of time by another independent witness. As a result any evidence produced by the victim will appear to be self supporting unsubstantiated evidence not acceptable to a Court.

This is a serious operational issue that has not been adequately addressed at present by the Community.

LINGO

Yet another legal issue that is emerging is one created by the use of different languages in the world and a desire to customize communication for best communication through internationalization and localization of content.

Some of the issues arising out of "International Domain Names" in non English format have already been discussed in the chapter on IPR/Domain Name Disputes. A related issue which is even more important is the use of non English language for the Content of a website along with "Automatic Language Translators" either as a server side software option or a client side Plug-in.

Providing a language web site understandable for those who know the language is a straight forward issue with fewer complications. In this case the responsibility for the content is entirely taken by the Content provider.

However, when the content is created in one language and is automatically converted into another, there is likely to be a distortion of meaning arising out of the conversion process. The

legal consequences arising out of such processes have to be determined based on "Who Has Created the Software", "Is it considered a Standard Software or not?", "Whose decision is it to use the software? Client's? Or Server's? etc.

Of late, "Lingo" as a concept of developing a new "Net Language" is gaining popularity as a standard Lexicon for localization of content. Localization is the process of adapting to meet the language, cultural and other requirements of a specific target environment or market (a "locale"). This process often entails the use of special computer-based tools. Localization involves translation (e.g. of manuals and other documentation, screens, help texts, and error messages). Equally, product names may have to be changed to avoid unfortunate associations in the target language.

In this context, internationalization is the "opposite" or forerunner of Localization. In other words, it is the process of designing and implementing a product, which is culturally, and technically as "neutral" as possible, and which can therefore easily be localized for a specific culture or cultures. This reduces the time and resources required for the Localization process, thus saving producers money and improving their time-to-market abroad. As with Localization, language, technical and contents issues are involved, with project management and coordination also playing a significant role. Internationalization has now reached the point where major software publishers can release as many as 30 different localized versions within a month or two of the original version, a process known as "simship" (short for "simultaneous shipment.

There is no doubt that Net Communication particularly the online Chat rooms and discussion boards have developed a lexicon of their own and many of the words and abbreviations used there in

are Greek and Latin to an ordinary Netizen. There is also no denying that the new terms developed by this Cyber Community have a distinctive meaning of their own.

However, complications arise in when some of these terms may get into digital contract documents, web pages or software usage terms and conditions. It is a standard practice in law to refer to Oxford or Chamber Dictionaries when there is a dispute on the meaning of any word. If the Lingo Lexicon is considered a popular reference source, there is no reason why Courts may not refer to www.netlingo.com or other similar web resources to interpret the intentions of contracting parties.

In the absence of a proper standardization and awareness of the usage of Lingo lexicons, some terms of a contract may be mis-understood by either party leading to possible avoidance of a contract or leading to an avoidable dispute.

Some times the Lingo lexicon may also clash with the legal terminology itself. One classical case is the Indian definition of the term "Hacking" which has been defined under Section 66 of the ITA-2000 while the Lingo lexicon defines a hacker thus:

> "A computer enthusiast who enjoys learning everything about a computer system and, through clever programming, pushes the system to its highest possible level of performance.. the term "hacker" tends to connote membership within a global community defined by computer networks; it implies that the person subscribes to some version of the hacker ethic. They use their hacking skills to develop penetration tools, and then they go out and analyze a customer's networks for security vulnerabilities, in order to report the findings back to the customer. Most hackers consider themselves something of

an elite (a meritocracy based on ability)"

This definition never contemplates "Hacker" as a "Criminal" while ITA-2000 is categorical about it. If therefore there is a document in which Mr X has admitted that he is a "Hacker" and it is produced in the Court as an evidence of admission of crime, it is possible that we may be dealing with the problem of "Lingo".

The solution for this is for parties to take care to have the section on "definitions" in all major contracts remembering that what a word may mean in Oxford or Chambers dictionaries may not be what the contractual party means.

In case such words are part of a web site as they are bound to be, then a hyper link from the "Disclaimer" page to an online Lingo dictionary may become a standard feature. Not doing so could be "Negligence".

For example, here is a foot note that may appear at the bottom of a Web page inviting you to become a member of the service.

"DIS SvC S 4 3 Mths 1ly"

This actually is a disclaimer that says "This service is for three months only". Probably, without a hyperlink to a website where this Lingo can be translated to plain English, it would be treated as an attempt to defraud the ordinary Netizen who cannot be expected to decipher these cryptic words.

SSH

Currently, almost all communications in computer networks are done without encryption. As a consequence, anyone who has access to a machine connected to the network can listen in on any communication.

This is being done by hackers, curious administrators, employers, criminals, industrial spies, and Governments. Some networks leak off enough electromagnetic radiation that data may be captured even from a distance.

SSL, HTTP-S and SET are some of the secure communication tools used by the industry for providing data security during transmission from one machine on a network to another. These work on the principle that the users at both ends have a digital ID that can be verified through a trusted third party certificate

One of the recent protocols that is coming to use is the SSH. SSH or Secure Shell is a program to securely log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecured channels. It is intended as a replacement for telnet, rlogin, rsh, and rcp. In SSH2, there is a replacement for FTP namely sftp. It is claimed that there are over 2 million Secure Shell users in over 60 countries indicating that it is fast emerging as a standard in its kind of use.

There is also a free version of the SSH protocol suite called Open SSH.

SSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other

network-level attacks. It provides protection against:

- IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host. SSH even protects against a spoofer on the local network, who can pretend he is your router to the outside.
- IP source routing, where a host can pretend that an IP packet comes from another, trusted host.
- DNS spoofing, where an attacker forges name server records
- Interception of clear text passwords and other data by intermediate hosts
- Manipulation of data by people in control of intermediate hosts etc.

In this context of "Avoiding Negligence", it is necessary for Network managers to evaluate the need for SSH in their organizations and document the reasons why it has been adopted or rejected in their organization.

DISTRIBUTED COMPUTING AND GENIE TECHNOLOGY

Yet another technology that poses difficult legal questions is the technology of Distributed Computing and Genie. The fundamental feature of these technologies is that the functional software derives its functionality from several components. The Consumer's end result derived out of the software is a function of the interactions of the various elements of computing. These components may be owned by different legal entities and work as "Agents" for specific purposes. They may also be located in different geographical areas in the world with different set of laws.

The legal accountability of such a software will have to therefore depend on several back-to back arrangements which may be either disclosed or undisclosed. The consumer may some times be confronted with a product which may actually be illegally tapping the services of a component and he may not even be aware of it. Whether this ignorance will constitute a valid defense or law will consider that the user has not exercised a reasonable care to determine the legality of the software delivered to him will be a matter which a court will have to determine on the basis of the circumstances of the case.

The Genie technology also operates on the principle of distributed functionality with agent components delivering critical data from one component to another which may trigger some the functionality of the components . These agents may also consist of some embedded hardware elements which gather environmental intelligence which is fed into a data base or an information system. The Decision making system may be triggered either by the information gathered by the intelligence system itself or by other decision parameters which may be default configurations or one which the user sets himself.

Under these circumstances, the performance of the hardware supported by the software using genie technology may depend on the performance of the genie agents. In case of any faulty performance of any of these agents, the end product functionality is again affected. When the genie applications run on the web, it is possible to conceive a situation where the different elements are owned and operated by different entities and disputes that may arise may have complicated inter play of warranties and norms.

One example of a genie functionality could be a stock market ticker which triggers an investment analysis and a stock buy decision, executed by an automated broker system and money debited to the Bank account.

Another example would be a drug administration system embedded within the body of a person which monitors the body functions and appropriately delivers drugs from the micro vials already embedded in the body or through other means.

In both these examples we can understand the criticality of the decision process and the dependency of the system on hardware and software items as well as the configuration at the user level. Any malfunctioning of the system either due to software bugs or through a corruption of the system, would lead to legal issues that are extremely complex to understand, argue in a court of law and judge. Anticipating legal issues that may emerge in such a situation and taking suitable remedial measures is an important aspect of protection both for the user and the service provider.

SOFTWARE CREATION TOOLS

The software development community today is using many tools that help them write codes for the software programme. They may be simple "Editors" or more complicated "Object Oriented Script Writers" or more sophisticated tools such as an Apache ANT or a Comprehensive application development environment such as Rational Rose. Some times the "Tools" may simply be pre developed library elements that are included as components into the product itself.

The functionality of the end product would obviously depend on the accuracy of these tools.

If there are any bugs in the software that pass through these tools or are a direct consequence of these tools, there will be an impact on the legal accountability of the user.

If suppose the developer has incorporated a "Disclaimer" disowning such liabilities or the consumer has directed that a certain tool can be or should be used, then there is a possibility of the accountability for bugs being shifted to the consumer.

A third angle to the software developed by the tools as opposed to direct code creation is that there may be unintended "Common patterns" in the codes which may clash with other similar products raising the issue of copyright.

Further the license terms of the tool supplier with the software developer may have an impact on the serviceability of the software in the long run.

Thus the software writing tools may bring in several legal complications to the software developer vis-à-vis the consumer.

SPEECH RECOGNITION AND CHARACTER RECOGNITION

Yet another area of technology development concerns Text to Speech, Speech to Text converters through appropriate recognition software. For example, a software may read out your mails through your mobile using text to speech converters or pick up your mobile phone message and deliver it to an e-mail address.

Here again the accuracy of the documents depend on the converters and some times the external factors such as the background noise levels. If disputes arise due to such factors it will be similar to contractual disputes arising due to the mistake of an appointed agent.

The legal accountability for an inefficient agent depends on whose agent he is. In any way such a device would be the agent of either the sender or the receiver.

At present it appears that these are special tools which parties will use with the full knowledge of the possible problems associated with them and hence would not result in legal claims.

WIFI AND THE SECURITY CHALLENGES

Wireless Fidelity or WiFi is the latest technology challenge to the Cyber regulation area. It is the technology that enables use of wireless devices to connect to Internet or to a remote computer. This has made it possible for a Lap Top or a hand held Personal Digital Assistant getting activated in an environment where Internet connectivity is available through a wireless signals.

When networks are connected by the wires , users are having a visual indication of connectivity. The lack of such visual clues to connectivity can enable any mischievous user of WiFi technology to hack into a nearby computer endangering the information assets belonging to innocent Computer users. The WiFi enabled Computer is in greater danger of being hacked into rather than a Computer connected to Internet since, the WiFi log in can directly provide access to the destination computer and all its open files unlike an Internet connection which normally terminates on the browser or the e-mail client.

In a widely WiFi enabled world it becomes a mandatory security requirement for every computer user to store all files in his personal computer in encrypted form and use a hardware token such as a smart card to activate and access his computer. Lack of such security discipline may be termed as negligence by the Computer user and dilute the legal rights of such a user.

IS IT ONLY A FANTASY? OR A REAL ISSUE?

We can recall that even now some would like e-mail contracts to be confirmed by paper confirmation. As long as Courts consider that the society has not adopted itself fully to use e-mails as the only communication with which contracts can be concluded, the practice of sending paper communications may be considered necessary.

Afterwards, non sending of paper confirmation will not amount to "Negligence". Similarly, the points made above in respect of some of the emerging technologies may not be considered sufficient for raising legal accountability at this point of time. However, in due course as more and more people start using the new technologies, they become established as practice and the legal issues that have been mentioned above will need to be recognized and acted upon. Otherwise it may be held as "Negligence" by one of the parties to the contract.

CHAPTER XXI

LEGAL ISSUES IN CYBER TAXATION

Taxation Laws are one of the most important legislations in any country since they affect all the citizens. Since Internet is a backbone for a new dimension of Economy, taxation of transactions in Cyber Space is a subject of interest to all Netizens.

In the early days of E-Commerce, some of the countries such as USA had specifically exempted E-Commerce from taxation as a measure of support to the developing area of business. Soon however, all Cyber transactions are expected to come under taxation.

In India a high powered committee on Electronic Commerce and taxation was constituted by the CBDT on December 16, 1999 under the chairmanship of Mr Kanwaljit Singh. The Committee has published a draft report for which public response has been sought and further announcements are expected.

While discussing Cyber Taxation, we need to discuss the taxation of income arising out of E-Commerce, Tax on Sales arising out of E-Commerce and Tax on Transfer of virtual properties and/or Rights there on.

MAJOR ISSUES IN CYBER TAXATION

The issues that need to be discussed regarding Cyber Taxation are

- ✓ Which Country Laws are to be applied for taxing Internet transactions given that the parties to the transaction and

the Server which facilitates the transaction are in different jurisdictions.

- ✓ How do we avoid Double Taxation?
- ✓ How do we recognize "Income" and "Property" in the virtual space?
- ✓ How do we treat Cyber Property and Cyber Wealth which are not converted into real world wealth?..etc

---

OECD PRINCIPLES

The Organization of Economic Cooperation and Development in at the OECD Ministerial Conference in Ottawa in 1998 agreed on the following key principles of taxation of E-Commerce.

- The present international norms for cross border taxation are capable of being applied to electronic commerce, but that some clarifications should be given as to how these norms, and in particular the Model Tax Convention, applies.

- The taxation should occur in the jurisdiction where consumption taxes place, and that the supply of digitized products should not be treated as a supply of goods.

- The information reporting requirements and tax collection procedures should be neutral and fair, so that the level and standard is comparable to what is required for traditional commerce (although different means may be necessary to achieve those requirements).

RECOMMENDATIONS OF HE KANWALJIT COMMITTEE

The Kanwaljit Committee has in its recommendations opined that there has to be uniformity in the taxation of traditional commerce and E-Commerce and to that extent there is no case for exemption of E-Commerce from Direct Tax.

The Committee also has recognized that there is no issue regarding domestic E-Commerce taxation except for the need to avoid evasion because of lack of records.

In respect of cross border E-Commerce however, the committee recognizes that there is a need to examine the incidence of tax and a mechanism to levy and collect the same.

Significantly, the Committee has come to the view that applying the existing principles and rules to E-Commerce is impractical and the concept of "PE" (Permanent Place of Establishment) adopted by few countries and backed by article 5 of the OECD model tax convention should be rejected.

The Committee has also expressed the view that an approach in the form of a low "Withholding tax" for any payment to a foreign enterprise with the option of being offset by tax on net income by the receiver in his country is a workable option. It has been recommended that CBDT should examine this option and the implementation mechanism.

The recommendations are awaiting clearance from CBDT and a detailed guideline is expected to be announced at the appropriate time.

E-COMMERCE TAX AS TAX ON E-SALES

The common understanding of E-Commerce is that a Company is using Web as a means of making sales and this results in profit, which is taxable. To the extent Web is a medium through which a "Brick and Mortar Company" can make sales, there is no problem in understanding the taxation aspects of "E-Sales".

The ITA-2000 is clear as to the incidence of Cyber Contracts, their place and time of execution. Hence, if Sales take place through the Net, it is not difficult to understand the implication of Sales or Income Tax. These transactions are taxable under the present provisions of taxation.

By the same principle, Sales through the web to foreigners are subject to foreign exchange regulations if any and the earnings can be treated as "Exports".

Purchase through the Web similarly from abroad amounts to "Imports" and is subject to foreign exchange and custom duty regulations as applicable.

THE AMBIGUITIES

While there is no ambiguity in the taxation of E-Sales the legal issues that surround Cyber taxation are interesting challenges to Taxation and Cyber Law observers.

Some of the issues that we need to discuss are,

What is the scope of "E-Commerce in the Taxation context?"

One basic aspect of E-Commerce refers to exchange of physical

goods through a contract that is concluded on the network. In this sense it is no different from E-Sales. In such sales, the goods are transmitted through physical means and have to pass through the physical barriers such as Customs and Excise counters. There is therefore a familiar point of control and taxation is not a big issue.

However, when the goods exchanged are digital files that can be downloaded online, there is no physical barrier that can act as a check point. The concern for taxation authorities in this case is the possibility of tax avoidance.

The real challenge comes when the service is say a "Music File" which is listened to online for a fee. In this case, it is only the "Experience" of the service that is transferred. One has to analyze the taxability of such a product say for "Sales Tax". Perhaps the existing provisions of Sales tax do not cover the sale of "Streaming Music Experience" as different from sale of Music in cassette or CD form.

Another grey area is when a software is sold as a "Shareware" with limited rights being transferred at the point of sale with a contractual understanding that if the file is kept beyond a trial period, then the sale will fructify otherwise the buyer undertakes to uninstall the software and desist from its use.

It may be possible in such a circumstance that the buyer either does not pay the sale consideration or pays only a limited amount for the trial period and continues to use it in default of his agreement.

A strict consideration of the present taxation laws would require that the seller has to show the sale as concluded and pay the sales and income tax on full proceeds while he has to show the amount

due as receivables. He should then request for a write off of the portion of receivables which is not realized. On the other hand if the merchant does not show the full value of the product or service, there is a possibility that the Income Tax assessment officer may treat the difference in value as "Suppression of Income".

It is therefore necessary for the Merchant to first of all adopt a "Cash" system of accounting and then invoice the service in such a manner that the value is split up into a limited period sale and renewal fees.

Just as "Delivery of Music" online is a property that is difficult to be classified as "Sale", if a content site provides access to some part of the site against a fee, then the sale is of the right to receive the information. Probably we can conclude that this is not subject to Sales tax.

TAXATION OF FREE SERVICE

Another area where confusion prevails in Cyber taxation is when services are given free for some specific motive.

In the simplest case the service may be given free because the user agrees to let advertisements be displayed while he is visiting the site. Or in exchange of his personal information for a marketing database.

Here there is a consideration that is passed on which is difficult to be valued at the point of sale and hence difficult to be taxed.

Another area of contention is the taxation of "Virtual Properties" of various kinds.

Internet Access:

For example, you buy access service from VSNL at Rs 750/- per 100 hours. Similar product may given free by another ISP such as caltiger.com. The concern is whether it is a deemed income in the hands of the recipient?

Indirect Donation

Another example could be of a site which donates say Rs 0.25 to a charitable organization every time you click on an ad. The difficulty is to determine if it is an income received and donated for a charitable cause. We cannot ignore it just because the amount involved is insignificant. It is a question of principle.

At the aggregator's end anyway the receipt is substantial. Should it then be considered as an income and a donation at their end?

Income on Domain Name Transfer

Yet another point of doubt is when some body purchases a domain name for Rs 400/- and transfers it for Rs 1 lakh. The point in question is What kind of property transfer is it and whether the value difference is to be treated as a Capital gain? Or Income?

Depreciation on Domain Name

Staying with the Domain names, we know that they can be booked from one year to 10 years at present. Therefore, if a company owns a "Domain Name", one issue that arises is whether the domain name cost can be depreciated over time.

Depreciation on Website

Another issue in depreciation is regarding the website. Let us say that an assessee has created a web site at an expense. Is it a revenue expenditure forming a current asset? Or Is it a capital expenditure until the site is formally launched and to be treated as a fixed asset for the Company? Can such a web site asset be attached by the Income Tax department? Are other issues to be sorted out.

Virtual Currency:

There are sites where you can earn "Coupons" or "Points" which are encashable on other sites. From the taxation point of view, it is necessary to clarify whether this is income earned, particularly if the earning is never converted into physical cash and is consumed in the Internet space itself for a virtual service.

Value of Virtual Content:

Virtual Content has a value and a Copyright. If this copyright is transferred or content shared, there is an exchange of value. This gives raise to a doubt whether this amounts to a taxable receipt. If so, we also have to clarify what expenses can be set off against such content sharing.

The issues in Cyber taxation are therefore many. It is expected that when E-Commerce Tax is introduced in India, there will be

clarifications on all these issues. Obviously, the problems will be so many that a separate section ahs to be added to the Income Tax Act if Cyber Taxation has to be introduced.

INCIDENCE OF SERVICE TAX ON CYBER TRANSACTIONS

In an administrative notification, the Ministry of Finance has announced that from July 16th 2001, any website which is collecting a fee for making its content available to the Netizens has to pay a service tax calculated at 5% of the amount so collected.

As a result of this provision, many sites in India such as Crisil.com, Icra.com, Capitalmarket .com, Cmie.com , lexsite.com, matrix.co.in, numtv.com, e-gurucool.com etc which have built in a revenue model for passing on value added content on a fee will now have to pay a service tax.

This taxation for content distribution raises an important legal issue of taxability of Cyber Speech. .

It is popularly believed that Internet is a medium of expression and web content is a form of speech. The Service tax therefore is similar to imposing a tax on listening to Cyber speech. If this is held valid, perhaps in future, any "Seminar" with participation fee would also be subject to a similar levy.

It must be recognized that the legal impact of this development will have implications on Cyber Jurisprudence in general and may be quoted as an accepted precedence elsewhere in the world. With international treaties on the Hague model being round the corner, it would not be long before the impact of this kind of legislation starts affecting Netizens in other countries outside India.

The Government of India has already brought the services of Cyber Café under service tax at the rate of 8% as per provisions of the budget 2003.

If therefore, a Cyber Café is using a dial up connection to connect to the ISP, then there is a service tax incidence on the Cyber Café in the telephone charges as well. Hence customers of such Cyber Café will be indirectly taxed twice under the head of Service tax.

CHAPTER XXII

CYBER WARS AND CYBER TERRORISM

We have already discussed in some detail, the different aspects of Cyber Crime in an earlier chapter. Cyber Wars and Cyber Terrorism are other forms of Cyber Crimes which need to be discussed separately.

Cyber Wars are attacks on the Cyber Property of a Government or any of its agencies by an enemy agent.

Cyber Terrorism is another form of attack where the Cyber property of civilians is attacked by an organized group which is inimical to the country.

Both Cyber Wars and Cyber Terrorism are "Organized" attacks coordinated for a "Common cause", as distinguished with Cyber Crimes which are attacks by individuals for a different motivation.

TYPES OF ORGANIZED CYBER ATTACKS

Like in the case of Cyber Crimes, we can look at organized Cyber Attacks in the following two different forms.

- Attacks on the Meta Society using Cyber Tools and
- Attack on Cyber Property in the Cyber Space.

CONVERGENCE OF WAR AND TERRORISM

War is an easily understood term in the sense that it is fought between one army and the other. "War" is not "Terror" since it is fought against the soldiers who are prepared for the fight and are equipped reasonably for the same.

On the other hand, Terrorism by definition is an act which creates wide spread fear amongst the general population. It threatens a large section of the civilian population not trained for or prepared for the war.

The key to Terrorism is the uncertainty of who will be the next victim. The objective of the attacker is to create panic and induce irrational self defeating behavior from the victim or his clan.

In recent days, the world is witnessing a blurring of distinction between a War and Terrorist Attacks.

Terrorism has now actually become a different form of "Warfare" itself. Just as "Guerilla Warfare" is a kind of war strategy, "Terrorism" has also become a strategy for "Proxy War".

Terrorism as a "Proxy war" weakens the enemy, makes him spread his resources thin over a large number of soft targets and creates vulnerabilities which the regular war can exploit.

Yet another reason why War and Terrorism appear to be converging is that today "Economic Warfare" is considered an effective complementary strategy to military warfare.

A weak economy starves the conventional war resources and makes the army weak and vulnerable by choking expenses on spare parts and war machinery.

The dependence of the current day army on technology also means that "Funds" to buy technology are today as important as "Men" to fight in the battle field.

Economic warfare has therefore become an important strategy in international warfare. Consequently, Cyber Terrorism has become a part of the strategy to disrupt the economy of the country through attacks from Cyber Space.

Since the concept of Cyber War and Cyber Terrorism are still in the emerging status, the two terms are often confused for each other and used an interchangeable. However we shall for the purposes of our discussions in this book try to distinguish the two and deal with them separately. We also shall recognize a variation of Cyber Terrorism in the form of Cyber Naxalism, where a part of the same society rebel against the authority and resort to means of destruction to express a view point.

LEGAL DEFINITION OF CYBER TERRORISM

The F.B.I. has defined Cyber Terrorism as

> "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives… through the exploitation of systems deployed by the target".

The above definition focuses on the objective of the attack and does not make a distinction between the Government and private property.

ITA-2000 AND CYBER TERRORISM

The Information technology Act has addressed specific issues relevant to Cyber Terrorism in two places.

Firstly, under Section 69 of the ITA-2000, the Controller can order "Interception" and "Decryption" of messages in the interest of the sovereignty and integrity of the nation as also to maintain friendly relations with the neighboring countries.

Secondly, under Section 70 of the Act, certain Electronic systems can be declared as "Protected Systems" and any attempt to unauthorisedly access such system may result in a imprisonment of up to 10 years.

Other than this, Section 66 on "Hacking" can be invoked in cases such as network intrusions and web site defacements and Section 65 can be invoked in case of tampering of computer records required to be maintained by law.

Unfortunately, the section on "Computer Contaminant" or "Virus" has been treated in the ITA-2000 only like a civil offence eligible for financial compensation only and if a Terrorist uses a Virus or a Trojan to perpetrate his terrorist activity, there is no adequate remedy for the state to book him for a criminal offence.

POTA AND CYBER TERRORISM

The Prevention of Terrorism Act-2002 (POTA) defines terrorism mostly with reference to the physical world since it focuses on the use of lethal weapons of destruction such as bombs, chemicals etc., causing death and physical destruction.

However, a close reading of the definition of "Terrorist Act " and "Property" used in POTA suggests that the act can be extended to Cyber Terrorism also.

For example, under section 1 (3) of POTA, Terrorist Act implies

Threatening the unity, integrity or sovereignty of India

- by any means whatsoever,
- in such a manner as to cause or likely to cause damage to or destruction of
    - property intended to be used for the defense of India or in connection with
    - any other purposes of the Government of India, any State
    - Government or any of their agencies

According to section 2 (d) of the same Act, "Property" includes assets of every description, whether corporeal or incorporeal, movable or immovable, tangible or intangible.

In view of the above provisions, POTA can be invoked when a Cyber Attack damages any property of the Government or its agencies.

POTA appears to be incapable of being invoked when the property involved is not belonging to the Government. In this respect, POTA does not cover Cyber Terrorism as defined by FBI.

In other words, POTA only applies to "Cyber War" against the Government of the day rather than Cyber Terrorism as we have defined distinctly.

USA PATRIOT ACT AND CYBER TERRORISM

Immediately after the September 11,. 2001 terrorist attack on USA, the US government enacted the Patriot Act to combat terrorism. It is interesting to note that this Act does cover many aspects of Cyber Terrorism.

The Act has mandated the setting up of a national network of electronic crime task forces, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

It must be noted that "Critical Infrastructure" and "Financial Payment Systems" which are largely "Electronic Systems" have been identified as "Targets" likely to be attacked by terrorists.

The Act also addresses the issues concerning "Money Laundering" connected with terrorist acts which are largely electronic transactions in the Cyber Space.

Thus the Patriot Act brings within its definition of Terrorism, attacks on private information assets also, which the Indian POTA has failed to do.

TARGETS OF CYBER WAR

Cyber war as we have defined, cover attacks on the Information Systems belonging to the Government. Some of the main targets in case of a Cyber war are

1. Information Systems of the Defense establishment such as the Missile Launching Systems or the Communication systems of the defense forces.

2. Information Systems of the Government agencies and ministries including their web sites.
3. Information Systems of vital nationally important scientific installations such as the Space programme, Weather Warning Systems etc.

For example, corrupting the information system that drives the Missile launch programme could be an objective of a Cyber War and it could be more effective than attempting to bomb the missile launch vehicle itself.

TARGETS OF CYBER TERRORISM

The targets for Cyber Terrorism on the other hand consist of the following.

1. Information Systems that control vital societal functions such as Electricity, Water supply etc. (Some of them may be controlled by the Government agencies, in which case they can be classified as coming under the category of Cyber War).
2. Information Systems that control Economic Functions such as the Banks and Stock Markets.
3. Information Systems and web sites belonging to the private sector companies.

The attacks in Cyber Terrorism may not necessarily always be a "Defacement of Website". What is more threatening is the modification of information in a website leaving the larger part of the website un affected so that the visitors are fooled into thinking that the alteration is genuine.

Examples of such subtle attacks could be a "Change in the Central Bank Interest Rate", a false " News report" about an "Assassination Attempt" of a political leader etc.

One of the live recent examples in India was an attempt to create panic amongst the customers of Global Trust Bank, a private sector bank in India and cause a "Run" on the Bank.

In a simple maneuver some of the customers of the Bank were sent e-mails stating to the effect that they should better withdraw their salaries deposited in the Bank quickly since the Bank may not be able to meet its commitments. This caused panic amongst a set of customers creating a Run on the Bank in a couple of branches. Fortunately, the Bank had enough strength to withstand the temporary run and weather the storm. Had the Bank not been sufficiently strong and buckled under pressure, we would have seen a Bank failure caused by a few e-mails resulting in irreparable losses to many individuals and organizations. This is the hallmark of a "Terrorist Attack"

> ..Using Simple Means, on Soft Targets and achieving maximum Devastation.

It is impossible for the Law enforcement authorities to prevent such happenings since it would not be practical to either prevent e-mails being sent across anonymously or to insist that every e-mail should be digitally signed.

It is reported that sending out of false e-mails was one of the strategies used in inciting communal violence during the 2002 Gujarat Violence.

Similarly, another long range tool used by Terrorists is the maintenance of "Hate Sites", such as www.dalitstan.org meant to sow the seeds of hatred and disharmony in the community. Some of these activities are very difficult to be curtailed since Law

cannot totally ignore the claims for "Freedom Speech" and "Human Rights". They require special innovative strategies which defeat the purpose of the Terrorists without affecting the "Freedom" of genuine citizens.

An example of such a strategy is the strategy suggested by naavi.com for neutralizing "Rogue Sites" such as www.dalitstan.org through a forced exposure of "Counter Views" to the target audience of these sites. Under this scheme it is suggested that visitors to sites declared by the Government as "Rogue Sites" would be first diverted to a "Cautionary Notice" through interception at the ISP level where the fact that the site is declared as a "Rogue Site", "The Reasons Thereof" and a link to the "Counter Views" are provided. The visitor would however be free to ignore these and enter the subject site. The mechanism is easy to implement and would ensure that the freedom of speech is not curtailed and at the same time, "Mis Information" cannot be sustained.

THE CHALLENGES FOR THE DEFENSE AGAINST ORGAINZED CYBER ATTACKS

The critical aspect of the threat associated with Cyber Attacks is the "Remote" nature of attacks. In executing the Cyber attacks, borders need not be crossed, Explosives or Chemicals need not be smuggled and placed and Terrorists need not keep their lives at stake.

In fact, the terrorist of tomorrow, may be able to do more with a keyboard than with a bomb". Attackers could wage cyber warfare from a computer anywhere in the world. In cases where the attacks are mounted from a territory hostile to the victim country, the tracing of the source of attack becomes even more difficult due to the lack of local investigative support.

Being an organized crime, the attacks in case of Cyber Wars and Cyber Terrorism are often supported by sophisticated technology tools that can camouflage the place of origin through effective IP spoofing and there is no earthly chance of conviction for the attacker in any international court of justice.

DEFENSIVE STRATEGIES

In the light of what we have discussed earlier, there is a need for a well conceived strategy against defending against Cyber Attacks. The strategy has to be worked around

1. Putting a "Protective Blanket" around the Information Assets to be protected
2. Using "Offense" as a means of "Defense". (Counter Cyber Terrorism)

Putting a "Protective Blanket" is essentially a " Network Security Issue" and should be handled through effective measures for Perimeter Security, Access Management Polices, hardware and Software Firewalls etc. The Rules accompanying the Information Technology Act 2000 has defined certain security guidelines for Computer Networks which can be considered as official guidelines. The Reserve Bank of India has also separately issued guidelines for Banks which amongst other things include the appointment of "Ethical Hackers" to monitor the security of Bank's Computer Networks.

CERT INITIATIVES

In dealing with the defense requirement against Organized Cyber Attacks, it is necessary to debate whether the Government has to assume any responsibility for defending the Information assets of the civilians including the corporate sector. At present, Governments do not seem to be prepared to accept any responsibility for the security of Computer networks in the private sector both for the reason that the private sector is better equipped to handle Computer security issues and also that the resources of the Government are limited.

In the long run however, the Government cannot abdicate the responsibility in protecting the Cyber Space of the country since the consequences of say the BSES computer network being attacked cannot be dismissed as an internal corporate affair.

Further, if the assets of a country's civilians are attacked solely for the reason that it belongs to a particular country means that the country has a responsibility to protect that asset. If we accept that "Economic Assets" of the country need to be protected in the larger interests of the Country, there is a need for the Administration to take some steps in the direction of protecting civilian assets being targeted by terrorists or enemy soldiers.

In order to provide such blanket cover, US started an initiative called "Computer Emergency Response Team" (CERT) as a collaborative effort between the Government, the Private Sector and Educational Institutions.
The CERT was conceived as an establishment from where technical assistance can be provided to the Information Asset Managers in case of Attacks and Threats.

As a part of its activity, CERT normally does " Security Related Research", "Keeps Incident Reports" and "Develops Security Solutions".

Today CERT initiatives have been taken up by many Governments all over the world. Some of the initiatives are being coordinated by Government agencies and some by Educational Institutions.

CERT IN INDIA

In India, a beginning has been made with the then public sector CMC Ltd taking up the responsibility at the instance of the Ministry of Information technology.

Accordingly, a Center for IT Security has been formed and it functions as the CERT in India through its website http://www.itsecurity.gov.in.

CMC has since been privatized with the Tata group acquiring the control interest and the future of this initiative is not clear.

If however the movement has to be taken to its logical operating levels, there is a need for greater private sector participation in the CERT activities so that the best resources are made available for this cause of protecting the Indian Cyber Space.

The Government of India in a recent notification given a special status to CERT-IND, the Indian operations of the US based CERT. This is a federally funded research and development center in USA operated by the Carnegie Mellon University.

CERT-IND is operating from the premises where the office of the Controller of Certifying Authorities situated in Delhi and is the nodal center for "Blocking of Websites".

It is also expected to assist Adjudicating Officers in respect of any Cyber Crime investigations if required.

COUNTER CYBER TERRORISM STRATEGIES

The difficulties in identifying and pursuing legal options to punish Cyber Terrorists is an impossible task. The passive defense strategy of installing more and more capable "Firewalls" to protect Networks is a strategy which is bound to be weak and ineffective.

One of the weaknesses of passive strategies of defense is that they are always "Reactive" in nature and bound to fail from time to time. In such cases of failure, damages are inflicted on the Information Assets and they have to be recouped. While the knowledge of the failure can be used to strengthen the security further, it always a step behind the technology of the attackers and the result is that the attacker has a long term advantage. A similar situation prevails on the ground in India where the "Terrorists" from across the Border continue to pound at India's soft targets and the retaliation is always relatively less effective.

It is therefore necessary for countries like India to develop an offensive strategy of protecting Information Assets of Indian Citizens. This requires development of a "Cyber Army" licensed to undertake Cyber War when necessary against those who practice Cyber terrorism.

This would destroy the Cyber Terrorism infrastructure of the attackers and increase their cost of carrying on the offensive.

Technically speaking, it is more feasible to counter a Cyber attack with a Counter offensive on the technically identified source of attack rather than identifying its Meta Society owners and taking legal action against them.

Just as in the real world situation, Punishing "Those who Harbor Terrorists" and "Those who Finance Terrorist Operations", is an effective means of undermining the terrorist operations, even in the Cyber Terrorism case, pulling down the web site of the terrorists and the ISP s who knowingly support Terrorist organizations is a legitimate strategy of Counter Terrorism.

Even though at first glance, an "Offensive Strategy" and the Concept of "Cyber Army" appears a drastic solution, many of the Governments world over are coming around to the view that it is a necessary path for effective Counter Terrorism strategies.

USA has already started a dialogue with many countries including India in formulating a global strategy for counter Cyber Terrorism and this should take shape in due course as a well rounded international strategy.

COUNTERING CYBER NAXALISM

Dealing with Cyber Naxalism is slightly different from dealing with Cyber Terrorism mounted from the sworn enemies of the country. Cyber Naxalites are those who have turned into rogue elements as a desperate form of protesting against what they believe is injustice.

Cyber Naxalites may by definition stay within the country and are available for legal prosecution if proper evidence can be gathered and perpetrators apprehended. Many of these Cyber Naxalites may however operate from behind Corporate networks and use spoofing techniques to divert attention. Considering the difficulties in countering an intelligent Cyber Criminal through legal means, it is even more difficult to counter the better organized Cyber Naxalites.

Strategy for Countering Cyber Naxalites is therefore more effective if the approach is to "Reform" rather than "Punish". One useful approach to practically implement this strategy is to use "Reformed Cyber Criminals and Naxalites" as a part of "Cyber Army" so that their skills are utilized for the benefits of the nation and they are positively motivated to use their dangerous skills for the benefit of the community.

It is necessary to monitor the effects of "Digital Divide" as the economy progresses and to prevent "Corruption" and "Nepotism" creeping into the Cyber Governance because these are the breeding grounds for the growth of Cyber Naxalism.

Indian law enforcement agencies are yet to understand and appreciate the Cyber Culture and Cyber Psychology of Criminals and the lack of such understanding is what can drive intelligent Computer programmers to becoming cyber criminals first and Cyber Naxalites next.
The Win-Win Strategy for Cyber Space Guardians of India is to convert these potential Cyber Criminals and Cyber Naxalites into Cyber Soldiers for the Country.

CHAPTER XXIII

CYBER LAW COMPLIANCY, THE NEED OF THE HOUR

Laws are enacted by the Parliament and notified in the Gazette for public information. Once a law is so notified, it is the responsibility of the society to understand what the law means and how to avoid digression of law. Ignorance is not considered a defense against any legal violation and hence the onus is on the citizen to be Law compliant.

Unfortunately, the Government often thinks that its responsibility in ensuring implementation of law ends with the enactment of a law. There is as a rule no follow up from the Government on the implementation of the law or a voluntary preparedness by the Government to spread the information about the law amongst the public.

In every session of the Parliament, several Bills are passed and except for the Finance Bill that comes with the Budget, no other Bill gets sufficient attention of the media for the public to get educated unless it is a politically sensitive Bill like the POTA..

It is strange that the Government does not think that it has some responsibility to ensure a system where by the salient features of any legislation reach the public.

Professional bodies such as the Associations of the Chartered Accountants, Company Secretaries and Industry organizations such as CII and FICCI conduct a few seminars here and there when the law is new and later forget it.

The legal profession is too preoccupied with its day to day functions so that it is left to the Law Colleges to introduce the new law in their curriculum in course of time for the community to slowly absorb the provisions of the law.

As a result, years role by without the public getting properly educated on the laws that shape their lives.

In the meantime some hasty implementation of the law by a law enforcement officer raises eyebrows and the poor law enforcement officer is blamed for not keeping with the developments of law which even the legal luminaries have failed to follow. Such actions also harass the innocent public making them feel bad about law in general and the Law enforcement machinery in general.

When a special law like the Information Technology Act which is having wide ramifications and also is complicated with its technology dependence gets enacted, the deficiencies of the system in not properly disseminating the law to the public get exaggerated.

This system of "Let the Citizen Beware" is a dangerous provision for honest Citizens who would like to be law abiding. The responsibility cast upon them to find out the details of the law, and get themselves educated is too burdensome.

Despite the difficulty however, Law Compliancy is a matter of extreme importance to the Corporate sector for the reason that the stakes in Non Compliance is too high.

BEING WISE AFTER AN EVENT

In the recent days, a quick glance around us indicate that there have been many corporate incidents that indicate the risks of Non Compliance of Cyber Laws.

Firstly, Radiant Software, a Chennai based IT training Company, faced the allegation that it was using a software in violation of the license terms. This resulted in the arrest of two of the executives of the Company, closure of some of the training centers, confiscation of the Computers and other equipments. The top executives were also threatened of arrest and prosecution on charges of Software piracy. Even though the company later settled the issue out of court, there was not only an unplanned financial burden on the company, but there was a permanent damage to the image of the company which made it impossible for it to continue in business.

Similarly, the Directors of Rediff.com and Times Of India faced the unwelcome prospect of being tried for "Distribution of Obscene Material" and imprisoned for up to 5 years.

Directors of a Web Hosting firm in Delhi were arrested for having removed a website form operation for alleged non payment of charges.

Several Companies running websites under their Corporate names or other names were stripped off their right to continue their web presence because the names they were using were confusingly similar to some other trade mark.
A Student of the Balbharati Vidya Mandir in Delhi was jailed for a few days and later rusticated from the school for posting obscene material on a web site.

A student from Pondicherry was arrested for Spamming a UK hosting firm. Some other students from different parts of Tamil Nadu and Andhra were arrested for sending threatening e-mails to VIP s.

The list of such events can only increase as the use Cyber Age progresses further.

Obviously no law abiding citizen wants to be at the receiving end of such incidents. More so if you are a Corporate head responsible for thousands of employees and millions of shareholders.
The only way we can ensure that we are not on the wrong side of the law is to develop a systematic approach to our Cyber lifestyle designed to avoid the crossing of the yellow line.

THE CONCEPT OF NEGLIGENCE

Negligence is a unique concept used in Law to determine the legal liability in certain cases where "Risk" in inherent in the nature of operations itself. For example, the "Risk of Explosion" in a Chemical factory is inherent in the nature of operations itself and cannot be eliminated completely. The management responsible for the safety of workers can only take reasonable care that can be taken under the circumstances to protect its workers in case of an accident.

The question of what is "Reasonable" is what determines the factor of "Negligence", i.e., not doing of a thing which a prudent man under similar circumstance would do or doing of a thing which a prudent man under similar circumstance would not do.

Obviously, this is a vague concept left to the discretion of the Judge in a given case based on the circumstances. Over a period of time certain principles of "Negligence" would evolve due to the repetitive nature of some crimes. Since the concept of "Negligence" imposes a responsibility for a "Dynamic Vigilance" and the IT is a field where significant changes keep happening every day, a Corporate Network Manager is always trying to hit a moving target of "Adequate Security" for the network.

What is important to note is that what is "Negligence" today may not be so tomorrow or vice-versa. Also opinions may remain divided on certain security issues. In such cases, it is the efforts taken and documented that will determine whether a Network Security Manager or the Company is negligent or not.

One of the ways by which a Company can document its intentions to be prudent is to undertake "Cyber Law Compliancy Exercises" at appropriate intervals with appropriate agencies.

THERE IS NO QUALITY WITHOUT COMPREHENSIVE CYBER LAW COMPLIANCY

In a Corporate environment, the risks of violation as well as the consequences of such violations are both high. It is therefore prudent for any responsible corporate management to minimize its Cyber Law Violation risks through a strict policy of Cyber Law Compliancy. This should be seen as a "Risk Management Principle" in the overall "Quality Standards of the Company".

The customers look forward to an uninterrupted service from the Company through out the life of the project and protection from unforeseen liabilities coming to them through the use of the Company's products and services. The ability to provide such a

product or service is therefore a "Quality Benchmark" for any Company.

Can you say if a Company cutting corners by using pirated software for its operations is a not a "Quality Risk"?. You never know when law will catch up with the company and it goes under just like Napster did.

Can you say if a Company using Electronic communications using insecure e-mails is not a "Quality Risk"?. You never know when the critical corporate information leaks to the competitors and undermines the existence of the Company.

Can you say if a Company using remote log in feature for their network without SSH (Secured Shell) implementation is not at "Quality Risk"?. You never know if the society of experts considers non implementation of SSH as "Negligence".

Can you say if a Company oblivious to the patent rights on one of their components is not a "Quality Risk"?. You never know when the Company would be hauled over the coal for infringement of patent rights.

Can you say if a Company without a proper Network security policy is not a "Quality Risk"?. You never know when a hacker would put critical third party data into a public message board wrecking the company's image and its coffers in terms of the compensation it is made to pay.

Can you say if a Company without a proper HRD policy for network usage is not a "Quality Risk"?. You never know when one of the employees ends up being a perpetrator of a Cyber crime that also lands the Company Directors in jail.

Whether it is "Hacking" or "Virus" or "Digital Contracts" or "IPR Rights", information assets of a Company are at risk of loss if the Cyber Law aspects are not adequately addressed. While no body can secure a Network 100 % through technology and accidents leading to loss of assets in therefore statistically unavoidable, a Company which is legally compliant in all respects can at least protect itself through Insurance or avoidance of liabilities.

Those Companies who think that Cyber Laws are only for lawyers to fight in a Court of law may die before the lawyer can start arguing.

It is imperative for any Company therefore to address all Cyber Law related risks that are relevant to their business and take such steps for prevention as a prudent man under similar circumstances would do.

COMPREHENSIVE CYBER LAW COMPLIANCY AS A REGULATORY TOOL

In countries such as USA and those belonging to the European Union, the process of Compliancy of Law is some times ingrained in the statute itself. For example the EU guidelines on "Privacy of Data" is protected by a mandate where by any Company belonging to the EU parting with such data to a processing house outside the Country is liable to be punished if the privacy of the data is not protected in the processing country through a due legal process.

Similarly, in USA, those companies who are handling health related information are bound by HIPAA compliancy and those who handle financial information are bound by GLBA compliancy.

These are examples of legal compulsions imposed on Companies so that they adhere to the requirements as enunciated in law.

Unfortunately, India does not follow such a policy of forcing the Citizens to follow certain legal standards in their own interests. The industry organizations who have recognized various Quality standards such as the ISO or CMM standards etc have not yet developed a sensitivity for Cyber Law Compliancy as a part of quality assurance standard.

As a result, it may not be impossible for a SEI CMM Level 5 company may suddenly realize that it has not provided for a Cyber Law risk which has resulted in a huge liability to the company and eroded its survival strengths. Remember that under the Information Technology Act, civil liabilities can go up to RS 1 crore for each victim. Just as the AAA rated Non Banking Finance Companies vanished from the scene due to non compliance of RBI laws, the SEI CMM and ISO rated Companies may find to their dismay that these quality assurances have not adequately covered the legal risks and have forced the Company into a false sense of security.

To prevent such a situation, it is the need of the hour for every Company either in the software or otherwise to establish a "New Quality Assurance Programme" which factors in the Cyber Law Compliancy Requirements.

THE PROCESS OF COMPREHENSIVE CYBER LAW (COMCYLAW) COMPLIANCY

The process of ComCyLaw compliancy involves the following processes:

- Cyber Law Risk Audit
- Cyber Law Risk Management Policy Formulation
- Cyber Law Compliancy Programme Development and Implementation
- Comprehensive Cyber Law Compliance Certification

CYBER LAW RISK AUDIT

Cyber Law Risk Audit is a study and identification of the Cyber Law Risks to which the subject Company is exposed. Such risks could arise due to the Computer Network used by the Company and also the Website, Intranet and Extranet systems maintained by it.

The audit covers stated policies of Network Security, Computer Usage, Password Management, Digital Signature Usage E-Mail Policy, etc.

It would also cover the policies of Data Back-up, Software Installation, Virus Management, Data Protection Measures etc.

It would also cover the policies for protecting the IPR of the Company as and when they are created.

The Cyber Law Risk Audit is documented and used as a bench mark for the implementation programme.

CYBER LAW RISK MANAGEMENT POLICY

Based on the findings of the Risk audit and after taking into account the business requirements of the Company and its clients, a Cyber Law Risk Management Policy Document has to be prepared to the satisfaction of all the stake holders of the Company.

CYBER LAW COMPLIANCY PROGRAMME

Once the Cyber Law Risk management policy is approved and a schedule of implementation is agreed upon by all the stake holders, a suitable implementation and monitoring programme would be developed and put into practice. Such programme includes Staff training, Regularization of Software Licenses, Checks and Balances to avoid accidental and inadvertent violations etc.

COMCYLAW COMPLIANCE CERTIFICATION

In order to remove internal biases that lead to unintended compromises, ideally an external agency should monitor the ComCyLaw Compliance and certify the current level of compliance and guide the Company for improving the compliancy to acceptable levels.

At present, Cyber Law Compliancy is a new concept which the corporate sector is trying to understand and Compliancy Certification Agencies are still in the development stage. The author is the pioneer in this concept on the global front and

working towards inclusion of Cyber Law Compliance within the quality assurance models of the established quality assurance programmes.

CHAPTER XXIV

INFORMATION SYSTEM SECURITY AUDIT

Cyber Law Compliancy Audit which was discussed in the previous chapter addresses the issue of compliance of Cyber Laws by a business entity. In the context of the Total security of Information Assets, it will be necessary to look at the security risks attached to Information Assets of a business entity which includes both "Technical Security" and "Legal Security".

In this chapter, we shall discuss some principles of Information Security Audit and the International Guidelines concerning the same.

The Information System Security Audit (ISSA) is relevant for all business entities having assets in the form of Information Assets stored either in the Network or on Removable Media.

The objective of the ISSA is to ensure that the information Assets of a business entity is protected against Unauthorized Access leading to loss or destruction of data or compromising of the confidentiality. Traditionally ISSA extends to preventive measures taken by an entity to gather intelligence that leads to mitigation of intrusion risks as well as the disaster recovery plans in case of loss.

The follow up action after data restoration through legal action against the intruder or defending oneself from legal liabilities arising out of the security breach is in the domain of "Legal Security" which is ensured in the Cyber Law Audit process.

Ideally speaking ISSA should cover "Techno-Legal Security Audit" rather than "Technical Security Audit Alone" and therefore Cyber Law Compliancy Audit should be part of ISSA.

However, at present since ISSA often tends to miss the Cyber Law Compliancy part, and focuses only on the technical security aspects we are addressing the two aspects of audit separately.

In the Indian context, the guidelines for Information System Security are contained in the schedule II of The Information Technology (Certifying Authority) Rules 2000. Though the rules appear to concern Certifying Authorities, since it has two distinct schedules namely Schedule II called the "Information Technology Security Guidelines" and Schedule III which is called "Security Guidelines for Certifying Authorities", it is reasonable to interpret Schedule II as the Statutory Security Guideline applicable to any Network in India relevant to determine whether the Network owner is exercising "Due Diligence".

Additionally, Reserve Bank of India has advised separate Security Guidelines for Networks in Banks.

Apart from drawing from the above guidelines, the general principles of ISSA briefly discussed here also conform to the standards of Information Security prescribed by OECD (Organization for Economic Co-operation and Development) as well as under the global standards such as IS17799/BS7799.

OECD has prescribed the following Nine Principles of Information Security:

1) Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance the security.
2) Responsibility: All participants are responsible for the security of information systems and networks.
3) Participants should act timely and co-operative manner to prevent, detect and to respond to security incidents.

4) Ethics: Participants should respect the legitimate interests of others.
5) Democracy: The security of information systems and networks should be compatible with the essentials of a democratic society.
6) Risk Assessments: Participants should conduct risk assessments.
7) Security Design and Implementation: Participants should incorporate security as an essential element of information systems and networks.
8) Security Management: Participants should adopt a comprehensive approach to security management.
9) Reassessment: Participants should reassess the security of information systems, networks and make appropriate modifications to security policies, practices, measures and procedures.

International Standards:

The evolution of the current International standards in Information Security started BS 7799 which was first published in 1995. It gave a code of practice for the implementation of security controls to protect information for Commercial organizations and Government departments.

In 1998 a second part to the standard was published, containing the specification for an Information Security Management system which allowed certification of an organization against the standard to be undertaken by a third party.

First part of the British Standard BS 7799 was revised in 1999 to incorporate changes in the business environment such as the growth in mobile computing and electronic commerce and the

developments in security controls for these issues. This was later issued in 2000, without many changes, as the international standard ISO/IEC 17799.

Part 2 of the standard was revised in 2002 to bring the format in line with existing management standards such as ISO 9001 and was renumbered to be consistent with the numbering used in ISO/IEC 17799.

ISO17799, is a detailed security standard. It is organized into ten major sections, each covering a different topic or area:

The ISO 17799/BS 7799 standards are divided into the following Ten main sections:

1. Business Continuity Planning:

The objectives of this section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

2. System Access Control

The objectives of this section are:

1) To control access to information

2) To prevent unauthorized access to information systems

3) To ensure the protection of networked services

4) To prevent unauthorized computer access

5) To detect unauthorized activities.

6) To ensure information security when using mobile computing and tele-networking facilities

3. System Development and Maintenance

The objectives of this section are:

1) To ensure security is built into operational systems;

2) To prevent loss, modification or misuse of user data in application systems;

3) To protect the confidentiality, authenticity and integrity of information;

4) To ensure IT projects and support activities are conducted in a secure manner;

5) To maintain the security of application system software and data.

4. Physical and Environmental Security

The objectives of this section are:

1) To prevent unauthorized access, damage and interference to business premises and information;

2) To prevent loss, damage or compromise of assets and interruption to business activities;

3) To prevent compromise or theft of information and information processing facilities.

5. Compliance

The objectives of this section are:

1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements

2) To ensure compliance of systems with organizational security policies and standards

3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

6. Personnel Security

The objectives of this section are:

1) To reduce risks of human error, theft, fraud or misuse of facilities;

2) To ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;

3) To minimize the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organization

The objectives of this section are:

1) To manage information security within the Company;

2) To maintain the security of organizational information processing facilities and information assets accessed by third parties.

3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

8. Computer & Network Management

The objectives of this section are:

1) To ensure the correct and secure operation of information processing facilities;

2) To minimize the risk of systems failures;

3) To protect the integrity of software and information;

4) To maintain the integrity and availability of information processing and communication;

5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;

6) To prevent damage to assets and interruptions to business activities;

7) To prevent loss, modification or misuse of information

exchanged between organizations.

9. Asset Classification and Control

The objectives of this section are:

1) To maintain appropriate protection of corporate assets and

2) To ensure that information assets receive an appropriate level of protection.

10. Security Policy

The objectives of this section are:

1) To provide management direction and support for information security.

Within each section are the detailed statements that comprise the standard.

NETWORK SECURITY FRAMEWORK

A typical Network Security Plan in an organization has the following four Security elements:

1) Perimeter/Physical Security

2) Network Security

3) Application Security

4) Document Security

The above functions are achieved through a combination of

Physical barriers such as locks, Gate Keepers, ID Cards, as well as Firewalls which control access to systems and applications as well as encryption to control document security.

Anti Virus and Trojan protection is part of this data protection process.

Where the document security or material security is critical, additional monitoring measures with the use of RFID tags (Radio Frequency Labels that can be affixed on a software or a document to monitor its movement)

Additionally, as a business continuity contingency plan, the Security Planner also undertakes to ensure that data is backed up frequently and can be restored quickly in case of damage due to a security breach. This disaster recovery plan may include backups on media and selection of safe locations to store the back up copies. Since such disaster recovery plans have to account for natural disasters also, physical separation of the main data and the back up is also a consideration for the Security planner.

Yet another extended objective of a Security Planner is to bring into use intelligent monitoring mechanisms (Intrusion Detection Systems-IDS).

A successful management of the Network security however depends on the implementation of the strategy in such a way that the productivity does not suffer. Having security that protects all the requirements of the business and yet not affecting the productivity of the employees or the convenience of the customers is a challenge which only the business manager can address and not the technical expert who erects the Firewalls.

It is for this reason that the Security Management is the ultimate

responsibility of the Business Manager and he needs to understand the challenges and the solutions available.

In order to successfully maintain the security parameters, it becomes necessary to audit the process periodically and introduce corrections that improve the security. It may be necessary in large organizations to have an effective Internal audit system and also a "Security Compliance Officer" different from the "Network Manager" in order to ensure complete protection of critical Information Assets.

From time to time, the internal auditors may require help in Cyber Forensics to spot and investigate frauds and collect necessary evidence in a manner that enables successful conviction in a Court of law.

The entire process of Network Security therefore consists of the following personnel.

- Technical Implementation Team
- Compliance Monitoring Person/Team
- Audit Team-Internal/External
- Forensic Investigation-Internal/External

In order to assist the Security Team with benchmarks to be followed, the Company has to develop Security Manuals consisting of a clear definition of the objectives and how they are expected to be supported by the staff. Lack of such manuals can be considered "Negligence" in terms of the legal accountability of the organization for Cyber crimes under Section 85 of the ITA-2000 and the liability of Network Service Providers under Section 79 of the ITA-2000.

In drawing up such manuals, guidance can be drawn from Schedule-II of the Information Technology (Certifying Authority) Rules and other industry level guidelines available.

Cyber Space Security..You Have a Role in it Too!

Just as in the Meta Space the responsibility of secreting the Citizens and their lawful assets falls on the Government that collects Taxes, it is reasonable to expect that those who Govern the Cyber Space who are expecting to tax the Netizen community should assume responsibility for the Cyber Space Security.

However, this does not mean that Government alone is responsible for the Cyber Space Security. After all, Security of the society consisting of many soft targets, cannot be ensured by the Government without an active cooperation from the public.

In ensuring security of Cyber Space, the public have two kinds of roles.

One is that of a responsible citizen who is vigilant to the happenings around him and bringing suspicious looking transactions to the notice of the appropriate authorities. This will help incident monitoring and early detection of major attacks.

As of now there is no apex agency of the Government in India to which a member of the public can report any abnormal happening in the Cyber space and it is the responsibility of the Government to create such an agency at the earliest..

Secondly, it is necessary for every Netizen to keep his own desktop secure. Negligent Netizens often provide the breeding ground for Virus dissemination and Distributed Denial of Services attack. This is where action is called for by individual Netizens in India.

Desk Top Security has several dimensions to it. Some of them are:

1. Anti Virus

Every Netizen needs to realize that today, a good Anti Virus programme is as essential to computer usage as an operating system itself. Hence, every Netizen should consider it mandatory to install a good Anti-Virus programme and keep it updated. While this may not guarantee 100 % protection against Virus attacks, this is the minimum responsibility that the society expects its constituents to follow.

The general observation is that more than the individual Home Computer user, there are many small and medium size enterprises who have inadequate security against Virus in the office network. This situation needs to be attended to at the earliest.

2. Firewall

In view of the possibility of hacker attacks and denial of service attacks using a weak system, it is necessary for every computer owners to install some form of personal firewall that provides a basic protection against unauthorised intrusion and extraction of information from the system.

3. Access Control

Whenever a Computer resource is shared either in the office or at home, it is necessary for the users to adopt a reasonable access security measure that ensures that only authorized persons log in to the machine and the activities of different users can be monitored if required with reference to their log in IDs.

Having introduced a log-in system, say a password authentication system, it is necessary to ensure that passwords are well configured

and often changed.

Passing on passwords to another person in an office should be made an act punishable under the employee regulations just as a Bank Manager cannot hand over the vault key to his subordinate except under a due process.

4. Digital Signatures

It is necessary for users to start using digital signature system at the earliest for authenticating outward messages as well as protecting stored documents against manipulation.

In the Indian context however, the digital signature infrastructure is still inadequate to meet the requirements of the individual users and it may take a while for proper user level applications to be available.

5. Application Security

After the passage of ITA-2000, every software application that runs on a Computer can be considered a legally appointed "Agent" of the Computer owner. Hence any activity of the software is attributable to the owner and this could lead to legal liabilities also.

One of the important problems that Indian Computer users are facing is that the application vendors are yet to realize the importance of security and sell applications that leave lot of security loop holes.

Additionally, most of the document processing applications and ERP applications sold by even large companies, are not "Cyber Law Compliant" and therefore present a risk to an unsuspecting user.

Selling ERP applications to companies without PKI infrastructure is a fraud on the consumer since in the event of a legal dispute the

documents generated by the system are not legally valid.

Before the advent of the Digital Signatures (i.e. before the passage of ITA-2000), it might have been acceptable to issue documents such as Bank account statements with the proviso "This is a computer generated document and does not require a signature". But any Bank issuing such statements now is violating the basic contractual requirement in Banking practice and is making a "False" statement.

There are also many e-governance applications which suffer legal validity because of not using digital signatures and pose a serious threat to the growth of computerization in India.

Before it is too late, application vendors should address the issue of making their applications "Cyber Law Compliant". Until such time, they must provide a statutory warning that "This Version of the Application does not support compliance of Cyber Laws in India".

Consumer activists may have to step in if applications that are non-Cyber law compliant are sold without alerting the consumer to the dangers he is being exposed.

Thus, we may conclude that the Netizen whether he is an individual or a corporate citizen, has a responsibility to maintain a certain level of Desk top security within the systems that he operates. This is like a requirement of a Car owner to keep his brakes in working condition before he ventures out into the public roads.

Netizens should also insist that any IT application that they purchase should be reasonably certified as to the legal compliancy aspect just as every Car manufacturer provides a deemed guarantee that it conforms to minimum safety standards and emission control regulations.

Compliance of such requirements should be ensured both through development of guidance notes by appropriate authorities and also through a positive incentivisation say in the form of "Insurance" against loss of information asset.

Simultaneously the Government should have a mechanism to advise the Citizens on Standard Software to use and develop a software certification programme from security point of view.

While CERT-India can be expected to contribute in this regard, a more appropriate organization for this purpose is the "Society of Electronic Transactions and Security" (SETS) which has recently set up its head quarters in Chennai and is well suited to meet the security requirements of the Cyber Society outside the Law Enforcement set up.

There is also a role for voluntary organizations such as the e-Information Systems, Security Association (e-ISA) in contributing to public education on Cyber Security and facilitating the security process.

Hopefully, "Desk Top Security" is adopted as a key project by SETS with the involvement of the private enterprises such as e-ISA and the cooperation of industry bodies such as NASSCOM, CII, FICCI and the Chambers of Commerce and contributions from Educational Institutions, both technical and non technical.

CHAPTER XXV

FAQ

FAQ is a common term that Netizens come across while surfing the Internet. It represents the Frequently Asked Questions that surfers have on any topic or site. Since while going through this book readers might come across many questions which might not have been explained earlier, this chapter on FAQ is provided. This Chapter contains some brief explanations of the terms and cases that a Cyber Law observer comes across. These are not meant to be exhaustive, technically perfect explanations but are meant only to provide an understanding of the underlying concept or issue.

WHAT DOES "CYBER" MEAN?

The origin of the word Cyber is attributed to the use of the word Cyber Space used by an author William Gibson in Neuromancer, a novel about a computer hacker. Cyberspace is the imaginary virtual space created connected computers in which communication takes place.

WHO IS A NETIZEN?

A citizen of the Cyber world. One who has an existence in the Cyber world with an identity. Just as a Citizen exists within a "Nation", the Netizen exists within the "Cyber Nation". Until Cyber space is not partitioned and brought under the control of different countries, Cyber Nation is global and without any geographical boundaries. It can however have technical boundaries.

HOW DID INTERNET ORIGINATE?

Internet originated from the project of the Department of Defense (DOD), USA, called ARPA (Advanced Research Project Agency) which was US president's response to Soviets launching the Sputnik in 1957 and testing of its first intercontinental ballistic missile. With the formation of NASA in 1958, ARPA moved away from aeronautics and focused mainly on computer science and information processing. ARPANET project was the world's first multiple-site computer network working on a common protocol. It was started with the objective of developing a communication technology which could survive partial destruction of telecommunication networks in the event of a nuclear war. The first network was created in 1969 between the participating universities UCLA (University of California, Los Angeles) and SRI (Stanford Research Institute). University of California, Santa Barbara and University of Utah then came into the network. In 1973, the first ARPANET international connection came into existence with University College of London (England) and NORSAR (Norway). This network gradually expanded reaching about 100,000 computers by 1989. As the public involvement in the Internet grew, the DOD gradually withdrew to the background and passed on the management of the Internet to the private sector.

WHO GOVERNS THE INTERNET?

Today Internet is effectively governed by ICANN which has control on the allocation of IP addresses and most of the domain names. It also controls the technical standards that drive the Internet. ICANN is a self regulated body with representations from many segments of the Cyber society. The legal aspects of the Internet are governed by the individual laws passed by different

Governments while WIPO exercises a substantial influence on the Intellectual Property rights connected with the Internet.

WHAT IS A PROTOCOL?

Protocol is the agreed format for transmission of data between two devices. It will determine how the device will identify the beginning and end of message, how they control errors, How to interpret different parts of the message etc.

WHAT'S TCP/IP

TCP/IP is a set of internet protocols that enable data to be sent across and received over the Internet. Both protocols were developed by the Department of Defense, Government of USA during the ARPANET (Advanced Research project.

Internet Protocol (IP) is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination IP address.

Transmission Control Protocol (TCP) is responsible for verifying the correct delivery of data from client to server. This Protocol breaks the data into convenient packets which are transported using the IP. When the packets are received at the destination, they are re assembled in the particular order using he packet identity and the original data is reconstructed. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

WHAT IS WORLD WIDE WEB?

World Wide Web or www is a system where different documents are formatted and stored on servers in the Internet so that they

can be accessed by any person connected to the computer and using a common application called the browser. The invention of the system is credited to a physicist Tim Berners-Lee

WHAT IS HTML?

HTML stands for Hyper Text Mark Up Language, the language for authoring documents on the World Wide Web.

WHAT IS BROWSER?

Browser is the application that enables reading of documents created in HTML language and is used for reading documents on the world wide web.

WHAT IS FTP?

FTP stands for File Transfer Protocol. It is a protocol used to upload files from a workstation to a FTP server or download files from a FTP server to a workstation. It is the way that files get transferred from one device to another in order for the files to be available on the Internet. Most FTP servers require the user to log on to the server in order to transfer files.

WHAT IS HTTP?

HTTP, is Hyper Text Transmission Protocol which is a protocol used to transfer files from a Web server onto a browser in order to view a Web page that is on the Internet. Unlike FTP, where entire files are transferred from one device to another and copied into memory, HTTP only transfers the contents of a web page

into a browser for viewing. FTP is a two-way system as files are transferred back and forth between server and workstation. HTTP is a one-way system as files are transported only from the server onto the workstation's browser.

WHAT IS POP3?

POP3 is the Post office protocol version 3 which is used for e-mail service. A pop3 identity such as naavi@vsnl.com is maintained at different domains such as vsnl.com and the protocol uses the IP address system to locate the domain and place the e-mails received for a given address. It can be retrieved by the addressee using any of the e-mail client applications such as outlook express or Netscape messenger.

WHAT IS SMTP?

SMTP stands for Simple Mail transfer Protocol which handles outgoing mails. The protocol is responsible for sending the mail to the respective domain contained in the address so that it can be placed in the pop3 box of the addressee.

WHAT IS IMAP?

IMAP stands for Internet Message Access Protocol developed by Stanford University for retrieving e-mail messages. Similar to POP3, IMAP sports some additional features such as Searching the messages for a Key word even while it is on the server.

WHAT IS UDP?

UDP is the short form of User Datagram protocol. It runs on IP networks like TCP and is used mainly for broadcasting messages. It offers a direct path to send and receive datagrams over IP network and is referred to as "Connection less Protocol".

In a Connectionless protocol the host delivers the message onto the network with the destination address, without establishing the connection with the destination machine. On the other hand, Connection oriented protocols such as TCP and HTTP first establish the channel of communication before delivering the message.

WHAT IS ASCII?

ASCII is an acronym for the American Standard Code for Information Interchange. It is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127. The standard is used for Computers to recognize characters.

WHAT IS TELNET?

TELNET is the terminal emulation programme for TCP/IP networks. It connects the user's computer to the server in such a manner that commands entered will work as if they are directly entered on the server screen. It is a common way to remotely manage servers.

WHAT IS XML?

Short form of Extensible Markup Language used for web documents. It is an improvement over HTML and allows designers to create their own customized tags.

WHAT IS MIME?

MIME stands for Multi Purpose Mail Extension and is a standard specification for formatting non-ASCII messages so that they can be sent over the Internet. This enables E-Mail clients to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

WHAT IS A HASH?

A hash is a number generated by a special process from a string of text . It is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value but the same text will always produce the same hash value. It is also one way in the sense that it is not possible to reconstruct the string of text given the hash value.

WHAT IS CRYPTOGRAPHY?

It is the art of changing text into a coded form so that the document can be kept confidential.

WHAT IS MD5?

MD5 is a hash algorithm created by Professor Ronald Rivest and is a standard system used to create digital signatures.

WHAT IS RSA?

The acronym stands for Rivest, Shamir, and Adleman, the inventors of the RSA algorithm which has become the de facto standard for industrial-strength encryption, of digital data.

WHAT IS SSL?

SSL stands for Secured Socket Layer which is a protocol used for secured exchange of data packets over the internet between the computer of the Netizen and a web site. SSL creates an encryption channel using an " Encryption Key for the Session" exchanged between the browser and the server.

WHAT IS SET?

SET stands for Secured Electronic transaction system that enables exchange of information between the Client computer and a Web server in the process of credit card authentication. SET uses encryption like SSL but it uses two sets of encryption so that information relevant to the merchant is encrypted with one set of keys and the information relevant to the online payment authorizing system to be encrypted with a different set. As a result the system ensures that information is made available to the merchant and the authorizer only on a "Need to Know Basis" and avoids the merchant receiving sensitive personal information of the client which can be misused at his end. SET also uses digital signatures to identify the user.

WHAT IS SSH?

SSH or Secure Shell is a program to securely log into another

computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

WHAT IS A PAYMENT GATEWAY?

Payment gateway is an online authentication mechanism for payments on a website using a credit card or any other similar fund source. It interacts with the online customer and on a real time basis verifies a reference database and authenticates the payment.

WHAT IS BANDWIDTH?

Bandwidth represents the amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

WHAT IS A COOKIE?

Cookie is a text file sent by a web server to the browser and stored in the user's computer. It enables the web site to identify the user when he re-visits the web site.

WHAT IS A CARNIVORE?

It is a programme ostensibly developed by FBI capable of monitoring Internet data traffic based on key words.

WHAT IS MAGIC LANTERN?

It is a software ostensibly developed by FBI and installed in target computers and capable of tracking the "Key Board Strokes " and

sending it to the FBI.

WHAT IS HONEY POT?

Honey pot is a trap set by the law enforcement authorities to lure a hacker.

WHAT IS A VIRUS?

Virus is a malicious executable programme which has the capability of propagating and reproducing itself and causing damage to the Computer in which it resides. Normally it enters a system when an infected programme is executed.

WHAT IS A TROJAN?

Trojan is a programme that enters a system in disguise and later harms the system or steals information on the system. It belongs to the Virus family.

WHAT IS A WORM?

Worm is a programme which moves from one computer to other through open communication channels. Having entered a machine it may exhibit either a Trojan like property or a virus like property.

WHAT IS A VANDAL?

Vandals are a new kind of a virus threat which often cannot be blocked by anti-virus software alone. In contrast to common viruses (which require a user to execute a program or open a file in order to cause damage), vandals are auto-executable

applications. Vandals can take the form of Java Applets, ActiveX controls, plug-ins, pushed content, scripting languages, or a number of new programming languages designed to enhance Web pages and email.

WHAT IS SPOOFING?

Spoofing is a method by which the IP address contained in a message sent by the Computer is altered so that the recipient thinks that the message has actually come from a different computer. Spoofing can also be done of the sender's e-mail address so that the recipient thinks that the mail has come from a different person.

WHAT'S A PLUGIN?

Plug in is an additional feature that is attached to a basic programme by means of an additional independent attachment to the programme. For example, the outlook express can be attached with a plug in to enable it resolve domain names provided by New.net.

WHAT'S NAPSTER?

Napster is a Company which was using a "File Sharing" technology to enable its subscribers to exchange MP 3 (A format used for music) files from one user computer to another. The service was hugely popular and had 20 million subscribers at one point. The Recording Industry Association of America (RIAA) went to the court stating that the service enabled violation of copyright and sought discontinuance of the service. Initial decision has been in favour of RIAA but the dispute is not yet considered closed.

WHAT'S YAHOO-NAZI MEMORABILIA CONTROVERSY?

The Yahoo-Nazi Memorabilia Controversy is a controversy on the jurisdiction of the French Court on the Cyber Space created by Yahoo. The dispute arose when the yahoo auction site listed some Nazi memorabilia for sale. The French Government objected to the sale as it was illegal in France for such a sale. Finally Yahoo agreed to remove the disputed sale from yahoo-France site but refused to remove it from the main yahoo site. The dispute is still in the courts.

WHO'S DMITRY SKLYAROV?

Dmitry Sklyarov was a Russian programmer working for a company called Elcomsoft. The company developed a software which enabled Adobe E-Books to be saved in a different format such as Word. Adobe objected to this software since it inter-alia, broke the software lock placed by Adobe on its file format disabling its conversion to any other format. Adobe invoked the DMCA (Digital Millennium Copyright Act) and arrested Dmitry Skylarov while he was visiting USA for attending a seminar since he was the chief programmer in Elcomsoft. The arrest raised lot of controversy on the subject and ultimately he was released. The case is presently being pursued on the Company.

ABOUT THE AUTHOR

NAAVI

Naavi is an E-Business Consultant based presently in Chennai, India. An Ex-Banker and a Financial Services Expert, Naavi worked as a Merchant Banker and a Financial Products Marketing Consultant for a better part of his long corporate career.

With the opening up of the Internet in India since 1995, Naavi turned his attention to the Internet media and since 1997 has been focusing on the harnessing of the Internet technology for business.

With a long teaching career in Banking behind him, Naavi turned his attention to Cyber Law Education in early 1998 itself when the draft E-Commerce Laws were contemplated in India. In the next few eventful years, Naavi had many pioneering achievements to his credit.

Naavi pioneered the first Cyber Law related website in India by converting his personal website www.naavi.com (Now available as www.naavi.org) into a Cyber Law information center in mid 1998. In December 1999, he authored the first book on Cyber Laws in India. In October 2000, he launched formal virtual courses in Cyber Laws through the dedicated Cyber Law Education center www.cyberlawcollege.com.

Through the next few years, Naavi launched www.verify4lookalikes.com a concept to relieve the Cyber world of substantial part of Domain Name disputes. He also launched the first Cyber Evidence Archival center in India through www.ceac4india.com trying to find solutions to many of the problems that arose in the Cyber Law Compliance area.

Release of the first E-Book in Cyber Laws from India was yet another pioneering achievement from Naavi.

Naavi is today a prominent Cyber Law Educationist in India and a member of some Advisory bodies related to Cyber Law regulation in India.

He is a regular guest faculty in a number of educational institutions including the School of Excellence in Dr Ambedkar Law University, Chennai and Police Training College Chennai.

Naavi assists Police when required in Cyber Evidence Collection and interpretation to judicial standards. He also offers services to Companies for conducting Cyber Law/Security programmes and Compliancy Consultancy.

Naavi can be contacted at naavi@vsnl.com.

For records, Naavi is the popular name by which Na.Vijayashankar is known, was born in Mysore, Karnataka,(India), is aged 50, and is a Post Graduate in Physics with Banking and Management qualifications.

BEFORE I SIGN OFF

After the release of the first version of this Book in 1999, the next book was released in E-Book form in May 2003.

However the community continues to favour the print version and since this title has been already noted as a reference book in the syllabus of several courses in Madras University as well as elsewhere, it was found necessary to make available a current version for the benefit of the students.

Suggestions if any may be sent to Naavi@vsnl.com.

Naavi

