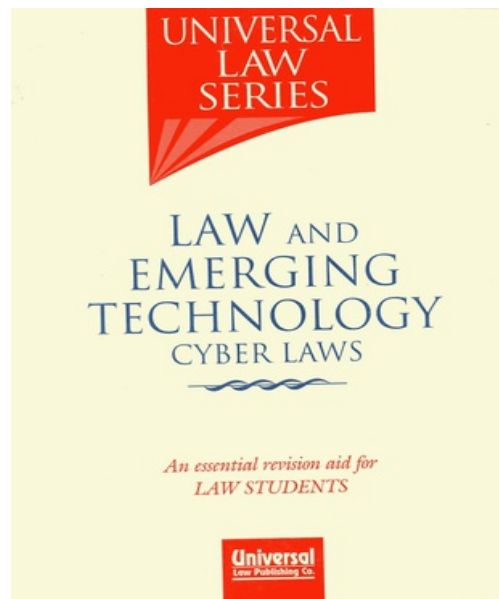
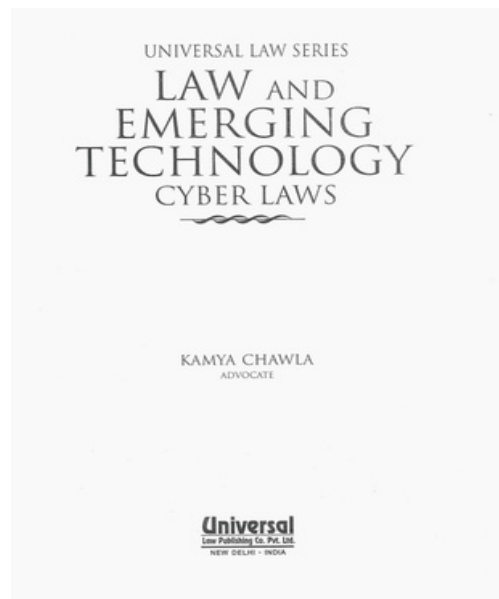


Toc



Authors Details

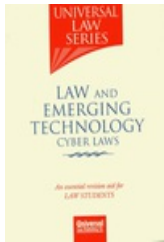
Toc



Contents

CHAPTER I

Introduction of Emerging Technology



• Overview	1
Q. What is Cyber Law?	2
Q. What is cyber space?	2
• Internet	3
Q. Who can make use of internet?	3

CHAPTER II

WORLD CHANGING TO E-COMMERCE

2.1 Introduction	4
2.2 History	5
Q. What is the Business Methodology of E-commerce?	5
Q. What is the legal definition of E-commerce?	6
Q. Write note on E-commerce and WTO?	6
Q. What are the main instruments of E-commerce?	6
Q. What is Business Process Re-engineering?	6
2.3 Online Approach of E-commerce	6
2.4 Case Law - Michel Dell Case	7
2.5 Types of E-Commerce Transactions in India	7
1. b2b (business to business)	7
2. B2C (business to customer)	7
3. C2C (customer to customer)	7
4. C2B (customer to business)	8
5. Non-business E-commerce	8
6. Intra-business (Organizational) E-commerce	8
2.6 Benefits of E-commerce	8
2.7 Benefits to Consumers	9
2.8 Benefits to Society	9
2.9 The Limitations of E-commerce	10
Technical Limitations of E-commerce	10
Non-technical Limitations	10
2.10 E-commerce - Changing Perceptions	11

CHAPTER III

M-commerce

•	Introduction	12
•	Mobile Phones	12
•	Payment Mechanisms on Mobiles	14
Q.	What are the various mode of payments on mobiles to avail various services?	14
•	M-marketing	15
Q.	Write a note on M-marketing?	15
•	Technologies of Mobile Phones	16

CHAPTER IV

Payment Mechanisms

4.1	Introduction	18
	Offline Payment System	18
Q.	Explain various modes of online payment system?	19
	Online Payment Sytem	19
4.2	Credit Cards	19
	Benefits to Customers	20
	Growth of Credit Card in India	20
	Debit Cards	21
	Different between Credit and Debit Card?	21
	Secured Payment Gateway (SPG)	23
	Secure Socket Layer (SSL)	23
	E-Wallet	23
	Mobile Payment	23
	Premium SMS Based Transactional Payments	24
	Mobile Web Payments (WAP)	24
	Smart Cards	25
	E-Billings	25
	Net Banking	26

CHAPTER V

DIGITAL SIGNATURE

•	Cryptography	27
•	Types of Cryptography	28

Advantage of Symmetric Cryptography	28
Disadvantage of Symmetric Cryptography	28
Advantage of Asymmetric Cryptography	28
Disadvantage of Asymmetric Cryptography	28
Q. What is digital signature?	28
Q. How digital signature is created and verified?	28
Q. Explain the statutory comparison between handwritten signature and digital signature?	29
Q. What is the relation between digital signature and asymmetric cryptography?	30

Chapter VI

Information Technology Act, 2000 - An Overview

Q. What are the main aims and objectives of I.T. Act, 2000?	31
Q. What is the Scope of I.T. Act, 2000?	32
Q. What was the micro and macro perspective of United Nations?	32
Q. Which countries join the digital signatures club membership?	33
• Extent of Information Technology Act, 2000	33
• Write a Note on Applicability of I.T. Act, 2000?	33
Q. What is the Jurisdiction of I.T Act?	33
• Attribution, Acknowledgment and Dispatch of Electronic Records	35
Q. What is secure digital signature?	36
• Regulation of Certifying Authorities	36
Q. Explain the appointment, function of the controller of certifying?	36
Q. Briefly describe the process of issuing, renewal, rejection, suspension of license of electronic signature certificates under the various provisions of law?	36
Q. What is the procedure to be followed by certifying authority?	37
• Disclosure - Section 34	38
Q. How the Electronic Signature Certificate Is Issued? Section 36	38
Q. How the Digital Signature Certificate is suspended? Section 37	38
• Revocation - Section 38	38

• Duties of Subscribers	39
Q. What are the various duties of subscribers?	39
• Penalties and Compensation for Damage to Computer, Computer System etc. - Section 43	39
• General Definitions - Section 43	40
• Penalty for Failure to Furnish Information, Return, etc. - Section 44	41
• Residuary Penalty - Section 45	41
• Power to Adjudicate - Section 46	41
• The Cyber Appellate Tribunal	41
• Procedure and Powers of the Cyber Appellate Tribunal (Section 58)	42

CHAPTER VII

Cyber Crime

7.1 Introduction	44
Q. What is computer crime?	44
7.2 Other Computer-related Offences	50
7.3 I.T. Critical Infrastructure in India	51
Protected System	51
National Nodal Agency	52
Indian Computer Emergency Response Team	52
Q. What is the Indian Computer Emergency Response Team? What are its function. What is the punishment for failure to comply with the directions of the Computer Emergency Response Team?	52
Q. What is the penalty for Breach of Confidentiality and Privacy?	52
Privacy in Indian Context	53
Q. Explain the concept of right to privacy along with leading cases?	53
Another Leading Case on "Right to Privacy"	53
7.4 Classification of Offences Against Other Laws	54
7.5 Classification of Cyber Offences	54
Penalty and Compensation for Damage to Computer, Computer System, etc. Section 43	54

Chapter VIII

Data Security and Data Protection

Q. Define computer Data Base?	57
Q. Write a note on UK's Data Protection Act, 1998? Explain its purpose also?	58
• Issue of Confidentiality	59
Q. What is the conceptual basis of confidentiality?	59
Q. Explain the main elements of confidence?	59
Q. Define what is the "confidential information"?	60
• Meaning of Confidential Information	60
• Confidential Materials	60
Q. Define what are confidential materials?	60
Q. What material is not included in confidential materials?	60
Q. What kind of restrictions are there on the receiving party to keep the information confidential?	60
Q. Explain the rights and remedies available with receiving party?	61

CHAPTER IX

Introduction to Satellite, Media, Cable TV, Broadcast

• The Prasar Bharti (Broadcasting Corporation of India) Act, 1990	63
• Section 2(a)- "Akashvani"	63
• Section 2(c)- "Broadcasting"	63
• Section 2(h)- "Doordarshan"	63
• Section 3-The Prasar Bharti Board	63
• Section 12-Functions and Powers of Corporation	63
• Section 13-Parliamentary Committee	64
• Section 14-Establishment of Broadcasting Council	64
• Section 23-Powers of Central Government	64
• Sections 32 and 33 Talks About the Rules and Regulations of Corporation	64
• The Cable Television Networks (Regulation) Act, 1995	65
• Section 2(aa)- "Cable Operator"	65
• Section 2(b)- "Cable Service"	65
• Section 2(c)- "Cable Television Network"	65
• Section 4-Registration as a Cable Operator	65
• An Overview of the Telecom Regulatory Authority of India	65

(Amendment) Act, 2000

- Section 14-Establishment of an Appellate Tribunal 66
- Section 14N-Transfer of Appeals 66

CHAPTER X

Domain Names and Domain Names Dispute Resolution

- Trademark 67
- Q. What are the rights of trademark owner?** 67
- Trademark Infringement 68
- Q. When it can be said that the owner of trademark is infringed?** 68
- Passing Off Action 68
- Q. What do you mean by passing off action? Explain its two broad categories?** 68
- Domain Names 68
- Domain Name Consist of Different Parts 69
- Domain Name Distribution 69
- Domain Name Infringements 70
- Q. What are the domain name infringements?** 70
- Resolving Domain Name Disputes 71
- Bad Faith Registration 72
- Q. What is bad faith registration?** 72
- Relevant Cases Related to Bad Faith Registration 72
- Q. How the distinctiveness is acquired? Explain with case laws?** 74
- Q. Write a note on WIPO?** 74
- Copyright and WIPO Treaties 75

CHAPTER XI

Advanced Technology

- The Protection of Plant Varieties and Farmers' Rights Act, 2001 77
- Important Definitions under the Act are as follows 77
- Section 2(j). Defines extant variety available in India 77
- Section 2(k). "Farmer" 77
- Section 2(l). "Farmers' variety" 77
- Section 2(za). "Variety" 77
- Section 12. Registry 78
- Section 13. National Register of Plant Varieties 78

• Chapter III of the act talks about registration of plant varieties and essentially derived variety	78
• Section 14. Application for Registration	78
• Section 15. Registrable varieties	78
• Section 16. Persons who may make Application	79
• Section 18. Form of Application	79
• Section 19. Test to be Conducted	79
• Section 21. Advertisement of Application	79
• Chapter IV of the Act Deals with Duration and Effect of Registration and Benefit Sharing	80
• Section 24. Issue of certificate of registration	80
• Section 26. Determination of Benefit Sharing by Authority	80
• Section 30. Researcher's Rights	80
• Chapter VI Talks about Farmers' Rights	80
• Section 39. Farmers' Rights	80
• Section 41. Rights of Communities	81
• Gene Fund	81
• Section 45. - Gene Fund	81
• Chapter VII of the Act Deals with Compulsory Licence	81
• Section 47. Power of Authority to make Order for Compulsory License	81
• Section 50. Duration of Compulsory License	82
• Chapter VIII of the Act Deals with Plant Varieties Protection Appellate Tribunal	82
• Chapter X of the Act Explains Infringement, Offences, Penalties and Procedures	82
• Section 64. Infringement by a Person	82
• Section 65. Suit for Infringement	82
• Section 66. Relief in Suit for Infringement	82
• The Biological Diversity Act, 2002	83
Q. Why biological diversity is creating?	83
Q. Explain the concept of bio piracy?	83
Q. Note on bacillus thuringiensis	84
Q. Overview of Act	84

Q. Who has to seek permission from the national biodiversity authority?	84
Q. Explain determination of equitable benefit sharing by NBA? In what manner it can be given effect?	85
• Chapter VI of the Act	85
• Chapters VII and VIII Talks About Finance, Audits and Accounts	86
Q. What are the duties of Central and State Governments mentioned under Chapter IX of the Act?	86
• Chapter X Section 41 of the Act deals with biodiversity management committee	86
Q. Write a note on biodiversity management committees?	86
• Chapter XII Miscellaneous	87
• Section 50 - Settlement of Disputes	87
• Section 55 - Penalties for Contravening Provisions of	87
Data Security And Data Protection	
• International Laws and Standards	88
• International Laws	88
• International Standards	88
• Data Privacy and Security Concerns in Outsourcing	88
• Why is data privacy and security one of the foremost concerns in outsourcing to India?	88
• How is India dealing with data privacy and security concerns?	89
• Proactive Data Privacy Measures in Indian Companies	89
• Data Privacy and Security Measures at Outsource2India	90
• Data Security at O2I: Process	90
• Data Privacy and Security: India Initiatives	91
• India as a Trustworthy Outsourcing Destination	91
• Introduction	91
• Understanding Data Security	91
• Threats to Organizational Data	91
• Solutions for Data Security	91
• Essential Components of an Information Security Management System	92
• Understanding Data Privacy	92
• Data Security v. Data Privacy	93

• Five Fair Information Practices	94
• Suggested Questions	95
• Table of Cases	97

© Universal law Publishing Co.

CHAPTER I

Introduction of Emerging Technology

Synopsis

Overview

Internet

Technological development is the process of research and development of technology. Many emerging technologies are expected to become generally applied in the near future.

The last decade has seen that the field of computer law has developed at a phenomenal rate in response to changing technology. Introduction to Computer Law explains the law clearly and makes it accessible to a wide audience. In this fourth edition, the law within the four key areas of intellectual property rights, contract, criminal law and data protection has been comprehensively updated, expanded and rewritten to reflect technological change, new decisions and new legislation. The emphasis is on describing and examining the law in the context of the practicalities of computer use. Introduction to Computer Law is suitable for under-graduate and professional students taking modules in the subject, and will also be invaluable to managers, computer professionals and legal practitioners.

Emerging technologies and converging technologies are terms used interchangeably to cover the emergence and convergence of new and potentially disruptive technologies such as nanotechnology, biotechnology, cognitive science, robotics, and artificial intelligence.

Overview

Many writers, including computer scientist Bill Joy, have identified clusters of technologies that they consider critical to humanity's future. Advocates of the benefits of technological change typically see emerging and converging technologies as offering hope for the betterment of the human condition. However, critics of the risks of technological change, and even some advocates such as trans-humanist philosopher Nick Bostrom, warn that some of these technologies could pose dangers, perhaps even contribute to the extinction of humanity itself; i.e., some of them could involve existential risks.

Much ethical debate centres on issues of distributive justice in allocating access to beneficial forms of technology. Some thinkers, such as environmental ethicist Bill McKibben, oppose the continuing development of advanced technology partly out of fear that its benefits will be distributed unequally in ways that could worsen the plight of the poor. By contrast, inventor Ray Kurzweil is among techno-utopians who believe that emerging and converging technologies could and will eliminate poverty and abolish suffering.

Internet is a path-breaking technological development which allows to operate and advertise across all frontiers and borders. Many companies offer various policies and schemes across the world through internet.

The main aim of cyber laws is to harmonize the existing laws. The cost of world wide transaction should be reduced by issuing inconsistencies and uncertainties arising out of difference in national laws. Many companies are expanding its business with great speed. With the development and increase in internet and electronic based trading system, the existing laws are getting affected. The traditional legal systems are facing difficulty in keeping pace with growth of internet and its impact. The Courts and Legislature will not be able to provide guidance in time to engage them in commerce.

The few statutory provisions have been enacted dealing with the problem of information technology laws. These laws are intellectual property rights (IPR). It seeks to remedy most of the problem. Because of the enactment of the IT Act the other Acts have also been amended to deal with some problems. These Acts are:-

❧• The Indian Penal Code, 1860

❧• The Indian Evidence Act, 1872

❧• The Bankers Book Evidence Act, 1891

❧• The Reserve Bank of India Act, 1934.

What is Cyber Law?

Cyber Law, includes legal, statutory and constitutional provisions which deal in computers and computer network.

The computers and the computer networks are used by any individual, corporate bodies and problem can arise to any body.

The cyber law applies to them only if-

1. Corporate bodies, institutions or individuals enter into cyber space.
2. They provide access to cyber space.
3. Creates hardware or software which enable people to access cyber space.
4. Use their own computers to go "online" and enter into cyber space.

The litigants in cyber disputes are telephone providers, companies, software companies, computer training institutes, schools, colleges, firms, etc.

What is cyber space?

Cyber space is nothing but a web of consumer where consumer electronics, their computers and communication network through internet are inter-connected in the world. The on-line world of computers and society that use these computers are included in the term cyber space.

Internet

Who can make use of internet?

For the access of computer and computer network, the term internet is necessary to understand. Internet is inter network of hundreds of other connecting networks made up of different types of computers all over the world where communications are made and messages are sent to each other using computers. Through internet, data such as video, pictures, sound and music, text are transmitted through satellite links and other media.

Internet can be used by any person at any place. Internet is also used for getting more information using various tools which are used to find out various resources on World-wide Web.

The research work using internet can be made in just few minutes or hours. Through internet, a person can also get knowledge of business world. One can also avail services like shopping, entertainment, banking, multimedia, etc.

The main role of internet is E-commerce. It means commercial transactions which take place electronically on internet.

It includes:-

1. Making Contract - In which parties while making contract on computers, signatures are put by parties on computers which is known as digital signatures. If there is breach of contract, the question of jurisdiction or law relating to breach of contract is regulated by cyber laws.
2. Buying and Selling - The persons doing shopping using internet are needed to be regulated by law. They do shopping using credit cards. The Domain Names of various sites are almost same, which creates confusion in minds of consumers e.g., RADIKK.COM and REDIFF.COM is same and it creates confusion. This needs to be regulated and our courts have held that these domain names should be used by original owner.
3. Publishing - It means copying or transmitting the work of author is violation of copyright. Downloading the work in any form i.e., printing, photocopying is violation of copyright and it needs to be regulated by law.

4.E-mail security - To protect the contents of e-mail it also requires to be regulated by law. Any misuse of cyber transaction is violation of law.

5.Banking and Advertising, etc. - Through internet the person can do banking on computer as it saves time of individuals, saves cost of transaction and it can be done at any time. Advertising is also done on computer which also saves time, cost, etc., and individuals are updated with new schemes on computer.

© Universal law Publishing Co.

CHAPTER II

WORLD CHANGING TO E-COMMERCE

Synopsis

2.1 Introduction

2.2 History

2.3 Online Approach of E-commerce

2.4 Case Law - Michel Dell Case

2.5 Types of E-Commerce Transactions in India

1. B2B (business to business)

2. B2C (business to customer)

3. C2C (customer to customer)

4. C2B (customer to business)

5. Non-business E-commerce

6. Intra-business (Organizational) E-commerce

2.6 Benefits of E-commerce

2.7 Benefits to Consumers

2.8 Benefits to Society

2.9 The Limitations of E-commerce

Technical Limitations of E-commerce

Non-technical Limitations

2.10 E-commerce - Changing Perceptions

2.1 Introduction

Electronic commerce, which is also commonly known as e-commerce or electric-commerce, is essentially the process of buying and selling of services or products over electronic systems like the Internet and various other computers, or any technology networks. The amount of business being done electronically has grown tremendously with the spread of the Internet.

Day-to-day examples of a wide variety of commerce conducted electronically, drawing and spurring on innovations in supply chain management, electronic funds transfer, online transaction processing, Internet marketing, inventory management, Electronic Data Interchange (EDI) systems, and automated data collection systems.

E-commerce includes conducting, managing and executing business transactions using modern technology.

The transactions of e-commerce are related to commercial activities between various organizations and individuals who are engaged in processing and transmission of data including text, sound and visual images.

E-commerce also refers to the exchanges of business ideas and information using electronic medium i.e., electronic mail, electronic fund transfer and other network based technology. It is not a manual process or paper transition but it is an electronic process which help the organizations and individuals to move forward and to change the technologies with ease.

Electronic commerce deals generally in the sales aspect of e-business. It sometimes also consists of the exchange of data in order to facilitate the financing and payment aspects of the business transactions.

Contemporary electronic commerce inculcates everything from ordering "digital" content for immediate online consumption, to ordering conventional goods and services, to "meta" services to facilitate other types of electronic commerce.

On the consumer level, electronic commerce is mostly conducted on the World Wide Web. An individual can go online to purchase anything from books, grocery to expensive items like real estate. Another example will be online banking like online bill payments, buying stocks, transferring funds from one account to another, and initiating wire payment to another country. All these activities can be done with a few keystrokes on the keyboard.

On the institutional level, big corporations and financial institutions use the internet to exchange financial data to facilitate domestic and international business. Data integrity and security are very hot and pressing issues for electronic commerce these days.

2.2 History

The use of electronic commerce has drastically changed over the last 30 years. Originally, e-commerce meant the facilitation of the commercial transactions electronically, i.e., use of technology such as Electronic Funds Transfer (EFT) and Electronic Data Interchange (EDI). Both of these were introduced in late 1970s, allowing businesses to transfer commercial documents like invoices and purchase orders. Moreover, the acceptance and growth of automated teller machines (ATM) and credit cards and telephone banking are also forms of electronic commerce. It was from 1990s onwards, electronic commerce started to include Enterprise Resource Planning Systems (ERPS), data mining and data warehousing.

Perhaps started from the Telephone Exchange Office, the earliest example of many-to-many electronic commerce in physical goods was the Boston Computer Exchange, a marketplace that used computers launched in 1982. The first online information marketplace, including online consulting, was likely the American Information Exchange, another pre-Internet online system introduced in 1991.

What is the Business Methodology of E-commerce?

E-commerce addresses the needs of traders, organizations, consumers and society. It reduces the cost of transactions while improving the quality of goods and services and also increasing the speed of services delivery.

What is the legal definition of E-commerce?

E-commerce is nothing but an exchange of goods and services for value on internet.

The Internet Tax Freedom Act, 1998, narrowly defines e-commerce as "any transition conducted over the internet or through internet access, comprising the sale, lease, license, offer or delivery of property, goods or services or information whether or not for consideration and includes the provision for internet access".

Therefore, any transition conducted over the internet by organization or an individual is called an e-commerce. It is also not necessary that the transaction conducted over internet is for some consideration or of free of cost. The essential element is that only the transaction should be conducted over internet.

Write note on E-commerce and WTO?

The World Trade Organization (WTO) is the only global international organization dealing with the rules of trade between nations. At its heart are the WTO agreements, negotiated and signed by the bulk of the world's trading nations and ratified in their Parliaments. The goal is to help producers of goods and services, exporters, and importers conduct their business.

The World Trade Organization is one of the largest organizations doing import and export business. With the development of technology and electronic world, Ministerial declaration on e-commerce defines it as "the production,

distribution, marketing, sales or delivery of goods and services by electronic means."

What are the main instruments of E-commerce?

According to World Trade Organization (WTO), the six main instruments of e-commerce are Telephone, Fax, Television, Electronic Payments, Money Transfer Systems, Electronic Data Interchange and Internet.

What is Business Process Re-engineering?

The Business Process Re-engineering is to create effective and efficient business process for better quality. The thrust of business process re-engineering is in managing the existing resources in optimum manner so that there is no wastage of resource. E-commerce is an example of business process

re-engineering, that is, to create effective and efficient business for better quality at lower cost.

2.3 Online Approach of E-commerce

Online approaches to perform traditional functions are:-

- 1.Payment and Funds transfers.
- 2.Order entry and processing e.g., in SMS form.
- 3.Invoicing i.e., through computer e.g., E-mails.
- 4.Inventory management - It means using software's i.e., the Bar code which has price, batch number of product, package, etc.
- 5.Electronic catalogues - every website is electronic catalogues e.g., customer care.
- 6.Point of sale data gathering - online sale is done by presenting online questionnaires or radio frequency, call centres, etc.
- 7.Advertising - online advertising of product is also an approach of e-commerce.
- 8.Marketing and customer support function - marketing through online medium or getting responses from customer is also an online approach.

2.4 Case Law - Michael Dell Case

In the year 1984, a person named as Michael Dell got a revolutionary idea in a hostel room. His idea was to sell PCs over the phone, rather than build a costly sales team or pay a middleman a distribution fee. In 1988, with great prices and quick delivery, Dell sales hit \$159 million. This model enables 30% gross margins and makes it easy for Dell to undercut rivals who enjoy 40% plus margin. They immediately went public and made an initial public offering and raised \$ 30 million. In the year 1995, the company reached new efficiency heights. Dell achieved the build-to-order system and providing services to customer from the level from 40 to 17 days. In the year 1997, Dell started its assault on the server business with models costing one-third as compared to rivals and jumped on the Net. By the month of April, it was doing \$1 million in sales daily online. Starting with 30 people it now needs 700 people to man the phones. In 1999, Dell sales increased to \$ 18 billion keeping its inventory to record low levels. In 2001, Dell became the No. 1 PC seller, with a 13% world-wide share. The profits were in \$ 361 million. In 2002, Dell consolidated its position over its nearest competitor HP by becoming the world's most widely distributed PC seller. Till 2003, as No. 1 PC seller in the world, Dell's company, currently holds 15% of the market share.

2.5 Types of E-Commerce Transactions in India

- Rapidly growing sector B2B (business to business sector).
- Low growth in B2C (business to customer sector).
- Stagnating C2C (customer to customer sector).

• Improving C2B (customer to business sector).

• Non-business e-commerce.

• Intra-business e-commerce.

1. b2b (business to business)

It involves the independent or dependent business entities. It is a deal maker, negotiator between these two entities. This is the case when two commercial organizations conduct some kind of commercial transaction using internet as an interface. e.g., Maruti Udyog - the biggest seller in world get ancillary parts from other business entities and assemble them.

2. B2C (business to customer)

This is the case when business entity being on one side hosts a site full of products and services for the customer. It is a retail version of e-commerce. It has web based shops. It makes shopping convenient for general people. Common examples of such sites are eBay, alibaba etc.

3. C2C (customer to customer)

This is the case when two or more customers involve with a business entity merely providing a web based interface to facilitate the customer to customer transaction. A very common example is amazon.com, where you get to see customer reviews which facilitate other customers about a specific product. It also includes customer to customer auctions. It is in realm of resale or rental. It creates market of second hand goods.

4. C2B (customer to business)

It is known as customer chaser or offering customers deals and packages at negotiable prices to customers. It is also known as "reverse auction". It is a business modal which is adopted by airlines, hospitably. It includes only barraging power. This category includes individuals who sell products or services to organizations, as well as individuals who seek sellers, interact with them and conclude a transaction.

5. Non-business E-commerce

An increased number of non-business institutions such as academic institutions, to-for-profit organizations, religious organizations, social organizations, and government agencies are using various types of e-commerce to reduce their expenses (e.g., improve purchasing) or to improve their operations and customer service.

6. Intra-business (Organizational) E-commerce

In this category, we include all internal organizational activities, usually performed on intranets that involve exchange of goods, services or information. Activities can range from selling corporate products to employees to online training and cost reduction activities.

2.6 Benefits of E-commerce

1. Electronic commerce expands the marketplace to national and international markets. With minimal capital outlay, a company can easily and quickly locate more customers, the best suppliers, and the most suitable business partners world-wide. A great example could be of the Boeing Corporation which reported a savings of 20 per cent. after a request for a proposal to manufacture a sub-system was posted on the Internet. A small vendor in Hungary answered the request and won the electronic bid. Not only was the sub-system cheaper, but it was delivered quickly.

2. Electronic commerce decreases the cost of creating, processing, distributing, storing, and retrieving paper-based information. For example, by introducing an electronic procurement system, companies can cut the administrative costs of purchasing by as much as 85 per cent. Another example is benefit payments. For the U.S. Federal Government, the cost of issuing a paper check is \$430. The cost of electronic payment is \$20.

3. Ability for creating highly specialized businesses. For example, stuffed toys which could be purchased only in pet shops or departmental and discounted stores in the physical world, are sold now on a specialized www.dogtoys.com, www.cattoys.com.
4. Electronic commerce allows reduced inventories and overhead by facilitating "pull"-type supply chain management. In a pull-type system, the process starts from customer orders and uses just-in-time manufacturing.
5. The pull-type processing enables expensive customization of products and services, which provides competitive advantage to its implementers. A classic example is Dell Computer Corporation.
6. Electronic commerce reduces the time between the outlay of capital and the receipt of products and services.
7. Electronic commerce initiates business processes re-engineering projects. By changing processes, productivity of sales people, knowledge workers, and administrators can increase by 100 per cent. or more.
8. Electronic commerce lowers telecommunications cost-the Internet is much cheaper than VANs.
9. Other benefits include improved image, improved customer service, newfound business partners, simplified processes, compressed cycle and delivery time, increased productivity, eliminating paper, expediting access to information, reduced transportation costs, and increased flexibility.

2.7 Benefits to Consumers

The benefits of E-commerce to consumers are as follows:

1. Electronic commerce enables customers to shop or do other transactions 24 hours a day, all year round, from almost any location.
2. Electronic commerce provides customers with more choices providing customers with less expensive products and services by allowing them to shop in many places and conduct quick comparisons.
3. In some cases, especially with digitized products, electronic-commerce allows quick delivery.
4. Customers can receive relevant and detailed information in seconds, rather than days or weeks.
5. Electronic commerce makes it possible to participate in virtual auctions.
6. Electronic commerce allows customers to interact with other customers in electronic communities and exchange ideas as well as compare experiences.
7. Electronic commerce facilitates competition, which results in substantial discounts.

2.8 Benefits to Society

The benefits of E-commerce to society are as follows:

1. Electronic commerce enables more individuals to work at home and to do less travelling for shopping, resulting in less traffic on the roads and lower air pollution.
2. Electronic commerce allows some merchandise to be sold at lower prices, so, less affluent people can buy more and increase their standard of living.
3. Electronic commerce enables people in Third World countries and rural areas to enjoy products and services that are otherwise not available to them.
4. This includes opportunities to learn professions and earn college degrees.
5. Electronic commerce facilitates delivery of public services, such as health care, education, and distribution of government social services at a reduced cost and/or improved quality. Health-care services, for example, can reach patients in rural areas.

2.9 The Limitations of E-commerce

The limitations of E-commerce can be grouped into technical and non-technical categories.

1. Technical Limitations of E-commerce.
2. Non-technical Limitations.

Technical Limitations of E-commerce

The technical limitations of E-commerce are as follows:

1. There is a lack of system security, reliability, standards, and some communication protocols.
2. There is insufficient telecommunication bandwidth.
3. The software development tools are still evolving and changing rapidly.
4. It is difficult to integrate the Internet and E-commerce software with some existing applications and databases.
5. Vendors may need special Web servers and other infrastructures, in addition to the network servers.
6. Some E-commerce software might not fit with some hardware, or may be incompatible with some operating systems or other components.
7. As time passes, these limitations will lessen or be overcome. Appropriate planning can definitely minimize their impact.

Non-technical Limitations

Of the many non-technical limitations that slow the spread of E-commerce, the following are the major ones:

1. **Cost and justification:** The cost of developing E-commerce in-house can be very high, and mistakes due to lack of experience may result in delays. There are many opportunities for outsourcing, but where and how to do it is not a simple issue. Furthermore, to justify the system, one must deal with some intangible benefits (such as improved customer service and the value of advertisement), which are difficult to quantify.
2. **Security and privacy:** These issues are especially important in the B2C area, especially security issues which are perceived to be more serious than they really are when appropriate encryption is used. Privacy measures are constantly improved. Yet the customers perceive these issues as very important, and, the E-commerce industry has a very long and difficult task of convincing customers that online transactions and privacy are, in fact, very secure.
3. **Lack of trust and user resistance:** Customers do not trust an unknown faceless seller (sometimes they do not trust even known ones), paperless transactions, and electronic money. So switching from physical to virtual stores may be difficult.
4. **Other limiting factors:** Lack of touch and feel online. Some customers like to touch items such as clothes and like to know exactly what they are buying.
5. **Many legal issues are as yet unresolved,** and government regulations and standards are not refined enough for many circumstances.
6. **Electronic commerce,** as a discipline, is still evolving and changing rapidly. Many people are looking for a stable area before they enter into it.
7. **There are not enough support services.** For example, copyright clearance centers for E-commerce transactions do not exist, and high-quality evaluators, or qualified E-commerce tax experts, are rare.

8. In most applications, there are not yet enough sellers and buyers for profitable EC operations.

9. Accessibility to the Internet is still expensive and or inconvenient for many potential customers. (With Web TV, cell telephone access, kiosks, and constant media attention, the critical mass will eventually develop.)

Despite these limitations, rapid progress in E-commerce is taking place. For example, the number of people in the United States who buy and sell stocks electronically increased from 3,00,000 at the beginning of 1996 to about 10 million at the end of 1999. As experience accumulates and technology improves, the ratio of E-commerce benefits to costs will increase, resulting in a greater rate of E-commerce adoption. The potential benefits and convincing reasons may not be enough to start E-commerce activities.

2.10 E-commerce - Changing Perceptions

- ✎• E-commerce has better information technology infrastructure.
- ✎• There is a wider acceptance of online payment system.
- ✎• There is also a legal recognition to E-commerce practices.
- ✎• There is an adoption of security standard by the industry.
- ✎• All the companies have moved to low value transactions on the net.
- ✎• It is not a new phenomenon. It is a business option that cannot be ignored in 'wired' or 'wireless' world.

CHAPTER III

M-commerce

Synopsis

Introduction

Mobile Phones

Payment Mechanisms on Mobiles

M-marketing

Technologies of Mobile Phones

Introduction

E-commerce relates to only business transactions and commercial process. E-commerce depends on the adaptation of new technology by the consumer, for the consumer and of the consumer. With the due development of technology and electronic world, world is changing to E-commerce and gradually to M-commerce. It was forecasted in 2007 that India will become the third largest mobile market by 2007. Common men have been lured by many offers e.g., life-time validity, free outgoing call within your network, free SMS, STD calls and ISD calls at very minimum rates, etc., which hooks the common man to the mobile world. Mobile is not just a phone, it has become an on-hand computer in which through an internet enabled mobile, people can receive e-mail, text messages. Mobile banking is also done through this. Railway booking, astrology, day to day news forecast facilities are available on the mobile phone, etc. The camera in mobile phones allows you to snap photos. Mobile phones are also used for investigative purposes. It is also forecasted that in future, in each and every case, mobile phones will be evidence in one form or another. From children to old men, every one is using mobile phones as it is helpful in locating persons.

Mobile Phones

Wireless telecommunication was the first step of cellular architecture. It was represented as basic like phones. Then at 2 G, digital technology was introduced. Earlier only voice communications were used in mobile phones but later with development of use of mobile phones and technology, data features like Short Messaging Service (SMS) was also allowed for the convenience of people. Then later at 2.5G, the most prevalent technology took place which has better software allowing increased data rates. At 3G, there is a greater widening of technology in which there are bigger data pipes for users allowing them more flow of information. Then later at 4G, the speed of multimedia delivery is very high with which the flow of information is also very high.

With the development of mobile world, it provides many advantages to common man:

- ✎• The devices are smaller in size. It is easy to carry anywhere and anytime.
- ✎• It has high mobility so a person can use it at any part of world since it has roaming facility at very nominal rates.
- ✎• It has better and permanent connectivity as one network is easily connected to another network. So it is easy for a common man to use any network and stay connected with other networks also.
- ✎• It has fast speed so a person can call another person any time in just few seconds.
- ✎• The service which is provided to common man is of a very high quality. Many features are provided in mobile phones to a common man with warranty and guarantee.
- ✎• The last but not least advantage of this technology is that it has very low cost as compared to other technologies. A common man can easily afford it and use it.

In an electronic world, website is used by customers for their personal use e.g., to access their accounts or business or to improve their business process.

Similarly, now the world is changing from E-commerce to M-commerce because instead of using websites on computer, all the practical applications are done on mobiles.

M-commerce is about-

✎• Personalization-Mobiles are made by common man for common man, it provides "made for me services" e.g., Ring tones, ring back tones, gaming, news update, gallery, etc. These services provided to a common man for their personal use and also a service of SMS/MMS is provided in mobiles so that in a short time a written message is sent to other person, if they don't have time to talk and also a message is sent through MMS in very short time. Mobiles also have a feature of real time responses.

✎• On demand-With the due development of this technology M-commerce is on demand. People want all information with ease. They want their personal information should also cope up with new demand. People want to access their personal data and personal software environment anytime anywhere on mobiles because it is difficult to carry computers or laptops as they are comparatively heavier than mobiles.

Mobile networks are fulfilling the urge of every human being as it provides data, personal software at any place and any time within few seconds.

✎• Micro payments-"micro payments" are defined as a financial payment in an amount which is related to a transaction cost that would incur in making the payment using traditional payment mechanism.

With the payment technology, it is easy to buy or sell low value digital products for small amount of money e.g., to download a ring tone software on mobile a very less amount is deducted from the balance. This system has increased the mobile commerce system.

With the development of mobile networks, desktop environment is changing into mobile environment.

Mobile networks are providing services and facility transfer of informative content to users in a short time and in efficient manner. Because of this application, the use of desktops is decreasing day-by-day. The stage of using internet on Desktops is shifting towards the stage of using internet in the palm of one's hand, i.e., mobile internet.

It is easy to access internet on mobile phones in a short time and in efficient manner.

For the use of mobiles by common man, focus is on the content. The manufacturers of mobiles are inclined to manufacture the product which provides satisfaction to customers. Many features are provided on mobiles:

✎• person to person video messaging

✎• Streamed videos

✎• News

✎• Sports

✎• Astrology

✎• Hi-resolution 3D games

✎• Entertainment

These features are provided on mobile phones for the entertainment of common man, so that they can enjoy with their mobile phones.

PAYMENT MECHANISMS ON MOBILES

What are the various modes of payments on mobiles to avail various services?

❧• Fee based-Every customer using mobile phones has to pay "fee" for downloading the pictures, songs or games, etc. The scheme is like "pay per view". The charges of downloading are very nominal and it can be paid either in form of cash coupons or the amount of fee is deducted from the balance amount of customer.

❧• Subscription based-The customer can also take subscription scheme on their mobile phones. They can take any scheme which they want and feel that it is convenient to use. The scheme must suit their budget also. The subscription amount is paid either monthly or quarterly or yearly, while taking schemes, many other free items like ring tones, limited amount of SMS, calls is also given to customers.

❧• Pay as you use-Other mode of payment for use of mobile phones is by recharging the phones with coupons. These coupons are easily available in the market and the person can recharge their mobile phones anytime, anywhere. After recharging with these coupons, the amount is deducted from the balance according to the calls made by the customers.

M-MARKETING

Write a note on M-marketing?

M-marketing is also a common phenomenon now a days. Every common man is inclined towards marketing of mobile phones. Sale and purchase of mobile phones is becoming a business. It provides employment to most of the people. Now courses have also been started to make mobile engineers.

M-marketing promises to provide-

❧• Cost effective-The cost of mobile phones is very nominal and it is easy for every man to afford it.

❧• Efficient-Every person can use the mobile phones efficiently. It is easy to use and easy to carry. Due to this feature, its demand is increasing day by day. Now it has become the need of every man.

❧• Precisely targeted-Every company of mobile phones has a target which they have to achieve. They are in competition with each other. And because of this competition they are offering many schemes at nominal charges to customers. Their target is only to provide satisfaction to customers.

❧• Ad-campaigns-It is the most common phenomenon in the business world. M-marketing also involves ad-campaigns in which they get profits. Through ad-campaigns, they get direct revenue from the advertisers who gain access to the operators customers. The revenue is generated from the users in responding back to the marketing campaigns. Revenue is also generated from transactions made by advertisers through their special offers and 'm-coupons'.

The survey is done on "ad-avoidance". It is conducted by BBC World and initiative media in various States in India. It is found that the survey of "ad-avoidance" is not common now-a-days after the increased use of mobile phones. It is found that "ad-acceptance" is highest in SMS and FM where the avoidance was just 14% and 24% respectively. The avoidance is only in the cable TV ads and magazines.

In the legal world, mobile evidence can be used to get relevant information:-

❧• It is used to locate a person or track a person's movements. For example, in a case of kidnapping, murder, and dacoity, it is easy to locate the criminal.

❧• It is used for fixing a person to a particular location at a particular time.

❧• Contacts in phone memory are also helpful in revealing the important information about person's link.

❧• Proving the criminal record of criminal activities of a criminal, by their outgoing and incoming calls and call duration.

❧• Pictures, videos, recording in mobile phones sometimes become a relevant evidence in proving the case.

TECHNOLOGIES OF MOBILE PHONES

The two main technologies of mobile phones are GSM which stands for Global Standard Communications and other one is CDMA which stands for Code Division Multiple Access.

❧• GSM technology-It was started in early 1980's. The development of mobile communications infrastructure was in 1990's. GSM service started in 1991. This year it was renamed as Global System for Mobile communications (GSM). More details about GSM can be taken on <http://www.gsmworld.com>

GSM network has three parts:

❧• Mobile Station (MS) - It is similar to the cordless phone with extra features.

❧• The Base Transceiver Station (BTS) - It controls the connection with the mobile station.

❧• The Base Station Controller (BSC) - It controls the Base Transceiver Station.

Mobile Station (MS) includes a digital mobile phone and a SIM card. SIM card is a silicon chip. The SIM (Subscriber Identity Modals) is a card that fits into the handset. The SIM contains identification details such as IMSI(International Mobile Subscriber Identity) which is numeric, where first 3 digits represent the country where the SIM is from and the other digits represent subscriber identity in phone memories, bill information, text message, PIN numbers.

An IMEI (International mobile equipment identity)is the serial number of GSM phone which is fixed in phone and cannot be changed.

❧• CDMA Technology - It has the great network capacity to serve more subscribers at same amount. It provides broad network coverage to all countries. It is a wireless technology and is a competing technology with GSM, TDMA, CDPD, etc.

In CDMA phones along with IMEI and IMSI numbers, ESN (Electronic Serial Number) and MIN (Mobile Identification Number) also identify the mobile phones.

❧• TDMA Technology - TDMA stands for (Time Division Multiple Access) which delivers digital wireless service. It combines data streams by assigning each stream a different time slot in a set. It transmits a sequence of time slots over a single transmission channel. It also combines PCM (Pulse Code Modulated) stream created for each conversation. It divides radio frequency into time slots and allocates slots to multiple calls. It is used by GSM digital cellular system.

❧• GPRS (General Packet Radio Service) - GPRS is used to send data at very high speed ranging from 9.6 kbps to 57.6 kbps by combining 3 to 6 voice channels of TDMA system.

❧• EDGE (Enhanced Data Rate for GSM Evolution) - It is a 3G technology based on GSM and TDM. It allows more data upto 384 kbps to be transmitted over TDMA radio frequency.

❧• Satellite phones - These phones are directly linked to satellite and do not have land based networks. It is similar to other phones. It also have prepaid connections which can be recharged from any part of the world. This phone is never out of coverage area because satellite can locate phone link anywhere on the globe. Satellite phone operators will have link with GSM networks because of cost effectiveness. It will also offer dual connectivity.

CHAPTER IV

Payment Mechanisms

Synopsis

4.1 Introduction

Offline Payment System

Online Payment System

4.2 Credit Cards

Benefits to Customers

Growth of Credit Card in India

Debit Cards

Difference between Credit and Debit Card?

Secured Payment Gateway (SPG)

Secure Socket Layer (SSL)

E-Wallet

Mobile Payment

Premium SMS Based Transactional Payments

Mobile Web Payments (WAP)

Smart Cards

E-Billings

Net Banking

4.1 Introduction

A payment is the transfer of wealth from one party (such as a person or company) to another. A payment is usually made in exchange for the provision of goods, services, or both, or to fulfil a legal obligation.

The payment mechanism is divided into two parts:-

1. Offline payment system.
2. Online payment system.

Offline Payment System

The simplest and oldest form of payment is barter system, the exchange of one goods or service for another. Barter, is defined as "a trade or exchange of goods or services without using money." Its origins are traced back to the dawn of mankind. Earlier bartering was done on a one-on-one basis and is still used today between some individuals and businesses on an informal basis. However, Modern Barter and Trade has moved beyond the old one-on-one barter concept by practising third party barter whereby the buyer is not obligated to purchase from the seller and vice versa. Rather, in Modern Barter and Trade, a barter exchange operates as a broker and banker and trade credits are used as a unit of exchange to facilitate trading among multiple companies and individuals. Modern trade and barter have developed into a sophisticated tool to help businesses increase their efficiencies by monetizing their unused capacities and excess inventories. The worldwide organized barter exchange and trade industry has grown to be an 8.0 billion

dollar a year industry and is used by hundreds of thousands of businesses and individuals as a mechanism to increase their revenues, preserve cash flows and market themselves to new buyers. The modern barter and trade industry operates to improve the overall economy by injecting additional commerce into the system and thereby improving the financial strength of all of its participants. The advent of the internet, and sophisticated relational database software programs has further advanced the barter industry's growth financial credibility. Barter offers a tremendous opportunity for entrepreneurs that understand economics, sales, banking and customer service. The U.S. Government officially recognized barter exchanges as third party record keepers in 1982 with the passage of the Tax Equity & Fiscal Responsibility Act which also required all barter exchanges to classify their members' barter sales as reportable income to the IRS via an annual 1099-B filing. Organised barter has grown throughout the world to the point now where virtually every country has a formalized barter and trade network of some kind.

In the modern world, common means of payment by an individual include money, cheque, debit, credit, gold, silver, paper currency or bank transfer, and in trade such payments are frequently preceded by an invoice or result in a receipt. However, there are no arbitrary limits on the form a payment can take and thus in complex transactions between businesses, payments may take the form of stock or other more complicated arrangements.

Explain various modes of online payment system?

Online Payment System

There are many modes under the online payments system. In this method, a third party must be involved. Credit card, debit card, money transfers, and recurring cash or ACH disbursements are all electronic payment methods. Electronic payment technologies are magnetic stripe card, Secured Payment Gateway (SPG), E-Wallet, Mobile Payment, Smart Cards, E-Billings, Net Banking etc.

4.2 Credit Cards

A credit card is a system of payment named after the small plastic card issued to users of the system. In the case of credit cards, the issuer lends money to the consumer (or the user) to be paid later to the merchant. Credit cards allow the consumers to 'revolve' their balance, at the cost of having interest charged. Most credit cards are issued by local banks or credit unions.

The credit card was the successor of a variety of merchant credit schemes. It was first used in the 1920's, in the United States, specifically to sell fuel to a growing number of automobile owners. In 1938, several companies started to accept each other's cards.

The card is issued by bank with different credit unions along with their logos (VISA/MASTERCARDS/DISCOVER/AMERICAN EXPRESS) are called acquirers who sign up with the merchants, while the banks are called issuers.

Credit card issuers usually waive interest charges if the balance is paid in full each month, but typically will charge full interest on the entire outstanding balance from the date of each purchase if the total balance is not paid.

Benefits to Customers

Because of intense competition in the credit card industry, credit card providers often offer incentives such as frequent flyer points, gift certificates, or cash back (typically up to 1 per cent. based on total purchases) to try to attract customers to their programs.

Low interest credit cards or even 0% interest credit cards are available. The only downside to consumers is that the period of low interest credit cards is limited to a fixed term, usually between 6 and 12 months after which a higher rate is charged. However, services are available which alert credit card holders when their low interest period is due to expire. Most such services charge a monthly or annual fee.

Growth of Credit Card in India

India is the second fastest growing market for financial cards in the Asia-Pacific region. The country's credit card

base, pegged at 27 million in 2007, is growing at an annual rate of 30-35%. The cardholders are increasingly using credit/debit cards for dining, purchasing clothing, petrol, durable goods and jewellery. Most Indians now have multiple cards, through which they utilize balance transfers to reduce their interest burden over the short term. A thriving economy, substantial increase in disposable incomes and consequent rise in consumer expenditure, growing affluence levels and consumer sophistication have all led to robust growth in credit cards, and each issuer has posted an enviable annual growth rate for several years. New products, foreign participation and a booming tourism industry are combining to create high levels of growth in India's nascent financial cards market, helped by product innovation and a supportive regulatory environment.

The number of credit and debit card users in India is climbing fast, and rising affluence is likely to erode Indians' lingering reluctance to spend on credit.

Indians have traditionally valued thrift and frugality. But the spread of affluence in the wake of rapid economic growth is challenging these values, at least for many middle-class and high-income families. One sign of this is the phenomenal growth in the number of credit and debit cards in India-in the past three years, the number of credit cards has more than doubled and the number of debit cards has almost quadrupled. However, despite these impressive rates of growth, the Indian market for financial cards is only beginning to show its enormous potential. Future growth will be driven by rising consumerism, intensifying competition among card issuers and an expanding financial architecture-although a culture of credit-based purchasing may take some time to develop.

Debit Cards

A debit card (also known as a bank card) is a plastic card which provides an alternative payment method to cash when making purchases. Functionally, it is similar to writing a cheque, as the funds are withdrawn directly from either the bank account (often referred to as a cheque card), or from the remaining balance on the card. In some cases, the cards are designed exclusively for use on the Internet, and so there is no physical card.

The use of debit cards has become wide-spread in many countries and has overtaken the cheque, and in some instances cash transactions by volume. Like credit cards, debit cards are used widely for telephone and Internet purchases.

Debit cards can also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash and as a cheque guarantee card. Merchants can also offer "cashback"/"cashout" facilities to customers, where a customer can withdraw cash along with their purchase.

Difference between Credit and Debit Card?

For consumers, the difference between a "debit card" and a "credit card" is that the debit card deducts the balance from a deposit account, like a checking account, whereas the credit card allows the consumer to spend money on credit to the issuing bank. In other words, a debit card uses the money you have and a credit card uses the money you don't.

In some countries: When a merchant asks "credit or debit?" the answer determines whether they will use a merchant account affiliated with one or more traditional credit card associations (Visa, MasterCard, Discover, American Express, etc.) or an interbank network typically used for debit and ATM cards, like PLUS, Cirrus (interbank network), or Maestro.

In other countries: When a merchant asks "credit or debit?" the answer determines whether the transaction will be handled as a credit transaction or as a debit transaction. In the former case, the merchant is more likely than in the latter case to have to pay a fee defined by fixed percentage to the merchant's bank. In both cases, the merchant may have to pay a fixed amount to the bank. In either case, the transaction will go through a major credit/debit network (such as Visa, MasterCard, Visa Electron or Maestro). In either case, the transaction may be conducted in either online or offline mode, although the card issuing bank may choose to block transactions made in offline mode. This is always the case with Visa Electron transactions, usually the case with Maestro transactions and rarely the

case with Visa or MasterCard transactions.

In yet other countries: A merchant will only ask for "credit or debit?" if the card is a combined credit+debit card. If the payee chooses "credit", the credit balance will be debited the amount of the purchase; if the payee chooses "debit", the bank account balance will be debited the amount of the purchase.

This may be confusing because "debit cards" which are linked directly to a checking account are sometimes dual-purpose, so that they can be used seamlessly in place of a credit card, and can be charged by merchants using the traditional credit networks. There are also "pre-paid credit cards" which act like a debit card but can only be charged using the traditional "credit" networks. The card itself does not necessarily indicate whether it is connected to an existing pile of money, or merely represents a promise to pay later.

In some countries: The "debit" networks typically require that purchases be made in person and that a personal identification number be supplied. The "credit" networks allow cards to be charged with only a signature, and/or picture ID.

In other countries: Identification typically requires the entering of a personal identification number or signing a piece of paper. This is regardless of whether the card network in use mostly is used for credit transactions or for debit transactions. In the event of an offline transaction (regardless of whether the offline transaction is a credit transaction or a debit transaction), identification using a PIN is impossible, so only signatures on pieces of paper work.

In some countries: Consumer protections also vary, depending on the network used. Visa and MasterCard, for instance, prohibit minimum and maximum purchase sizes, surcharges, and arbitrary security procedures on the part of merchants. Merchants are usually charged higher transaction fees for credit transactions, since debit network transactions are less likely to be fraudulent. This may lead them to "steer" customers to debit transactions. Consumers disputing charges may find it easier to do so with a credit card, since the money will not immediately leave their control. Fraudulent charges on a debit card can also cause problems with a checking account because the money is withdrawn immediately and may thus result in an overdraft or bounced checks. In some cases, debit card-issuing banks will promptly refund any disputed charges until the matter can be settled, and in some jurisdictions the consumer liability for unauthorised charges is the same for both debit and credit cards.

In other countries: In India, the consumer protection is the same regardless of the network used. Some banks set minimum and maximum purchase sizes, mostly for online-only cards. However, this has nothing to do with the card networks, but rather with the bank's judgment of the person's age and credit records. Any fees that the customers have to pay to the bank are the same regardless of whether the transaction is conducted as a credit or as a debit transaction, so there is no advantage for the customers to choose one transaction mode over another. Shops may add surcharges to the price of the goods or services in accordance with laws allowing them to do so. Banks consider the purchases as having been made at the moment when the card was swiped, regardless of when the purchase settlement was made. Regardless of which transaction type was used, the purchase may result in an overdraft because the money is considered to have left the account at the moment of the card swiping.

Secured Payment Gateway (SPG)

As the internet increasingly becomes the hunting ground for snoopers and scammers, secure communication are essential, Secure Payment Gateway, using the Secure Socket Layer (SSL) technology allow Gateway, Card holders, Merchants, Processors and others to encrypt and safely communicate sensitive and confidential data over the web.

Secure Socket Layer (SSL)

A small electronic file that uniquely identifies individuals and servers on the internet. Secure Socket Layer certificate the web browser to authenticate an internet site before entering confidential information such as user name or password. Typically, Digital Secure Socket Layer certificate are issued by "certification authorities" who are trusted and independent parties that ensure validity.

E-Wallet

A digital wallet (also known as an e-wallet) allows users to make electronic commerce transactions quickly and securely.

A digital wallet functions much like a physical wallet. The digital wallet was first conceived as a method of storing various forms of electronic money (e-cash), but with little popularity of such e-cash services, the digital wallet has evolved into a service that provides internet users with a convenient way to store and use online shopping information.

A digital wallet has both a software and information component. The software provides security and encryption for the personal information and for the actual transaction. Typically, digital wallets are stored on the client side and are easily self-maintained and fully compatible with most e-commerce web sites. A server-side digital wallet, also known as a thin wallet, is one that an organization creates for and about you and maintains on its servers. Server-side digital wallets are gaining popularity among major retailers due to the security, efficiency, and added utility that it provides to the end-user, which increases their enjoyment of their overall purchase.

The information component is basically a database of user-inputted information. This information consists of your shipping address, billing address, payment methods (including credit card numbers, expiry dates, and security numbers), and other information.

Mobile Payment

Mobile payment (also referred to as mobile web payment or WAP billing) is the collection of money from a consumer via a mobile device such as their mobile phone, SmartPhone, Personal Digital Assistant (PDA) or other such device.

Mobile payment can be used to purchase any number of digital or hard goods, such as:

- ❧• Music, videos, ringtones, games, wallpapers and other digital goods.
- ❧• Books, magazines, tickets and other hard goods.

There are two primary models for mobile payments:

- ❧• Premium SMS based transactional payments.
- ❧• Mobile Web Payments (WAP).

Mobile payment solutions have been widely adopted by a wide range of leading companies, for example World Wrestling Entertainment for the sale of audio and videos.

Premium SMS Based Transactional Payments

This is where the consumer sends a payment request via an SMS text message to a shortcode and a premium charge is applied to their phone bill. The merchant involved is informed of the payment success and can then release the paid-for goods.

Since a trusted delivery address has typically not been given, these goods are most frequently digital with the merchant replying using a Multimedia Messaging Service to deliver the purchased music, ringtones, wallpapers, etc.

A Multimedia Messaging Service can also deliver barcodes which can then be scanned for confirmation of payment by a merchant. This is used as an electronic ticket for access to cinemas and events or to collect hard goods.

Transactional payments have been popular in Asia and Europe but are now being overtaken by mobile web payments (WAP) for a number of reasons:

1. Poor reliability - Transactional payments can easily fail as messages get lost.
2. Slow speed - Sending messages can be slow and it can take hours for a merchant to get receipt of payment. Consumers do not want to be kept waiting more than a few seconds.

3.High cost - There are many high costs associated with this method of payment. The cost of setting up shortcodes and paying for the delivery of media via a Multimedia Messaging Service and the resulting customer support costs to account for the number of messages that get lost or are delayed.

4.Low payout rates - Operators also see high costs in running and supporting transactional payments which results in payout rates to the merchant being as low as 30%.

5.Low follow-on sales - Once the payment message has been sent and the goods received there is little else the consumer can do. It is difficult for them to remember where something was purchased or how to buy it again. This also makes it difficult to tell a friend.

Mobile Web Payments (WAP)

This is where the consumer uses web pages displayed on their mobile phone to make a payment. This process is quickly replacing premium SMS based transactional payments for digital content and also enables the sale of physical goods. Using a familiar web payment model gives a number of proven benefits:

- 1.Follow-on sales where the mobile web payment can lead back to a store or to other goods the consumer may like. These pages have a URL and can be bookmarked making it easy to re-visit or share with friends.
- 2.High customer satisfaction from quick and predictable payments.
- 3.Ease of use from a familiar set of online payment pages.

Mobile web payment methods are now being mandated by a number of mobile network operators. A number of different actual payment mechanisms can be used behind a consistent set of web pages. Mobile payment systems are also used in developing countries for micropayments.

Smart Cards

A smart card, chip card, or Integrated Circuit Card (ICC), is defined as any pocket-sized card with embedded integrated circuits which can process information. This implies that it can receive input which is processed - by way of the ICC applications - and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally PVC, but sometimes ABS. The card may embed a hologram to avoid counterfeiting. Using smart cards also is a form of strong security authentication for single sign-on within large companies and organisations.

A "smart card" is also characterized as follows:

- ✎ Contains a security system with tamper-resistant properties (e.g., a secure cryptoprocessor, secure file system, human-readable features) and is capable of providing security services (e.g., confidentiality of information in the memory).
- ✎ Asset managed by way of a central administration system which interchanges information and configuration settings with the card through the security system. The latter includes card hotlisting, updates for application data.
- ✎ Card data is transferred to the central administration system through card reading devices, such as ticket readers, ATMs, etc.

E-Billings

Electronic Billing (General) is the electronic delivery and presentation of financial statements, bills, invoices, and related information sent by a company to its customers. Electronic billing is also known as other payment models based on consumer-to-business and business-to-business:

- ✎ EBPP - Electronic Bill Presentment and Payment (typically focused on business-to-consumer billing and

payment).

❧• EIPP - Electronic Invoice Presentment and Payment (typically focused on business-to-business billing and payment).

Electronic bill payment is a fairly new technique that allows consumers to view and pay bills electronically through internet. There are a significant number of bills that consumers pay on a regular basis, which include: power bills, water, oil, internet, phone service, mortgages, car payments, etc. Systems send bills from service providers to individual consumers via the internet. The systems also enable payments to be made by consumers, given that the amount that appears on the e-bill is correct. Many banks are offering these online payment services for some time now, and are growing in popularity.

Net Banking

Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.

Online banking solutions have many features and capabilities in common, but traditionally also have some that are application specific.

The common features fall broadly into several categories-

❧• Transactional (e.g., performing a financial transaction such as an account to account transfer, paying a bill, wire transfer... and applications... apply for a loan, new account, etc.).

❧• Electronic bill payment.

❧• Funds transfer between a customer's own checking and savings accounts, or to another customer's account.

❧• Investment purchase or sale.

❧• Loan applications and transactions, such as repayments.

❧• Non-transactional (e.g., online statements, check links, cobrowsing, chat).

❧• Bank statements.

❧• Financial Institution Administration - features allowing the financial institution to manage the online experience of their end users.

❧• ASP/Hosting Administration - features allowing the hosting company to administer the solution across financial institutions.

© Universal law Publishing Co.

CHAPTER V

DIGITAL SIGNATURE

Synopsis

Cryptography

Types of Cryptography

Advantage of Symmetric Cryptography

Disadvantage of Symmetric Cryptography

Advantage of Asymmetric Cryptography

Disadvantage of Asymmetric Cryptography

A digital signature is a block of data at the end of message. It provides the identity of a person who has applied the signature.

The Information Technology Act aims to provide legal recognition for transaction carried out by electronic data interchange and other means of electronic communication. The other means is electronic filing of documents with the government agencies. Thus, Information Technology law is creating standards to control the electronic impulse. Public key infrastructure is created by organizations to create trust in their network system and security policies. It is also known as public key cryptography. Digital Signatures are the public key cryptography which can be used to make internet communications and data stored in internet safer with growth of internet and its impact. The Courts and legislators will not be able to provide guidance in time and to engage them in commerce.

The advantage of public key infrastructure is the production of software, and software integrity verification added with virus protection. The other main benefit of this technology is to provide data integrity. The main benefit of digital signature is that the modification of electronic form is not possible. The information is stored and protected by digital signature. Digital Signature is also highly important to the e-governance and e-commerce.

Cryptography

People are using cryptography to protect the data and messages. Cryptography is used to prevent criminals from reading confidential letters, memo, reports, etc. Cryptography is a kind of secret writing which helps in storing information and which can also be revealed to those who wish to see it and it can be hidden from all others.

It involves two processes:-

• Encryption Process - It is a process where the text message is encrypted into an unintelligible form.

E.g.: Message - "Reaching Delhi on August 24"

Encrypted Message:

ASDFGHJKMNBVCXSDRTYUJNBVCXDFGH

• Decryption Process - It is the process where the message in unintelligible form is decrypted into an 'original' text message.

E.g.: Encrypted Message

ASDFGHJKMNBVCXSDRTYUJNBVCXDFGH

Decrypted Message

"Reaching Delhi on August 24"

Types of Cryptography

1. Symmetric Cryptography - In this type of cryptography, only one key is used to encrypt and decrypt the message. It is also known as private-key cryptographic system.

Advantage of Symmetric Cryptography

• Only two parties are involved : Sender and Receiver of the message.

• It is cheaper than the public key systems.

Disadvantage of Symmetric Cryptography

The key which is used by both the parties i.e., sender or receiver of message can be misused by any third party (HACKER).

2. Asymmetric Cryptography - In this type of cryptography, two keys are used. One key is used to encrypt the message and another key is used to decrypt the message. It is also known as public cryptography system.

Advantage of Asymmetric Cryptography

• That no key is required for sender and receiver to transport the secret key over communication channels.

• That there is involvement of a trusted third party "Certifying Authority".

Disadvantage of Asymmetric Cryptography

• It is suitable for short messages only. It is not suitable for bulk encryption where megabytes of data is required.

• Public key system is expensive.

What is digital signature?

A digital signature is block of data at the end of message that attests to the authority of the file. It is necessary to note that if any change is made to the file, the signature will not verify.

How digital signature is created and verified?

A digital signature is created and verified by cryptography in which the message in an electronic form is converted into an unintelligible form and when it is received by receiver of message, it can be converted into original form.

The new Oxford dictionary defines digital signature as "a person's name written in different manner as a form of identification in authorizing a cheque or any document."

Legally, a signature means visible form of writing which has some evidentiary attributes like signers approval, identity, etc.

Explain the statutory comparison between handwritten signature and digital signature.

Statutory Criteria	Handwritten Signature	Digital Signature
Purpose	To authenticate the message as originating from the purported signer.	To authenticate the message as originating from the purported signer.
Affirmative Action	The written content is bound by legal implications of signing.	An electronic record is bound by legal implications of affixing.

Evidence	Distinctive, attributable to signer only.	Distinctive, attributable to signer only.
Signer identification	Witness/notary	Trusted third party, notary does not identify the digital signature.
Document identification	It is impossible to alter the signed or the signature without detection.	Non-repudiation, i.e., preventing a person from modifying or terminating the legal obligation arising out of transaction made through computer.

The digital signature becomes legally binding to the signer (sender) when:-

- 1.The certifying authority (Trusted Third Party) is a licensed one.
- 2.A digital signature has been created as per the technology standards prescribed under the law.
- 3.The digital signature verification process has become successful.

The main purpose of digital signature is that it identifies the signer of an electronic message and also assures that the signer approved the content of that electronic message.

Comparison between electronic signature and digital signature:-

Criteria	Electronic Signature	Digital Signature
Definition	It refers to all the methods by which one can 'sign' an electronic record.	It is technology specific type of electronic signature.
Technology	It can be created by using different technologies, it also satisfies the requirement of a legal signature.	It involves public key cryptography (asymmetric cryptography to sign a message).
Legislative examples	There are different statues which have been enacted in the various countries like Australia, Austria, Bermuda, Canada, Germany, Japan, Hong-Kong, Malaysia, Singapore and European Union, etc. (E-sign Federal enactment have been enacted in South Korea, UK as 'electronic signature' legislation).	Technology specific statutes have been enacted in various States of the United States. Various countries like India, Argentina, Italy, Columbia have enacted 'digital signature' legislation.

By the 2008 amendment of the Information Technology Act, 2000, the words "digital signature" were substituted by the words "electronic signature" in some sections and chapter.

It uses "Public Key Cryptography" in which two different keys are mathematically related.

What is the relation between digital signature and asymmetric cryptography?

One key is used for creating a digital signature and converting the message into an unintelligible form. Another key is used to verify the digital signature and transforming the data into original form. This process is known as Hash Function.

Two parties are involved in this two-way process of Digital Signature.

• The signer (creator of digital signature).

• The recipient (verifier of digital signature).

The process of digital signature is complete only when the recipient receives the message and verifies it.

What is the process of digital signature?

There are two process involved in Digital Signature:-

• Creating a digital signature - It is a process in which the message is typed in computer and the limited information is to be signed and termed as "message". The hash function in the signer's software computes the hash result which is unique to the message and the message is then transformed (encrypts) by the hash result into the digital signature using the signer's private key. The digital signature is unique to the message and the signer's private key. The digital signature is then attached to the message and it is stored with the message. Signer sends both digital signature and the message to the recipient.

• Verifying the digital signature - When the receiver receives the message along with the digital signature and receiver applies the signer's public key on the digital signature and recovers the hash result from digital signature. The hash result of the original message is computed by way of hash function which is used by signer to create the digital signature. The hash result should be same if so computed by the verifier and so extracted from digital signature. If the hash result is not same, then it means that it is altered or originated elsewhere after it was signed and the recipient can reject the message.

© Universal law Publishing Co.

Chapter VI
Information Technology
Act, 2000 - An Overview
Synopsis

Extent of Information Technology Act, 2000

Write a Note on Applicability of I.T. Act, 2000?

Attribution, Acknowledgment and Dispatch of Electronic Records

Regulation of Certifying Authorities

Disclosure - Section 34

Revocation - Section 38

Penalties and Adjudication - Section 43

General Definitions - Section 43

Persons Required under the Act - Section 44

Residuary Penalty - Section 45

Power to Adjudicate - Section 46

The Cyber Regulations Appellate Tribunal

The I.T. Act, 2000 is first kind of Legislature created in the Indian legal system. It came into existence on 17th October, 2000.

I.T. Act, 2000 has three main features:-

1. An enabling Act - It is known as enabling Act because it enables the regime of electronic signatures.
2. Facilitating Act - It facilitates e-commerce and e-governance.
3. A regulatory Act - It regulates cyber crime and other cyber related offences.

What are the main aims and objectives of I.T. Act, 2000?

The main aims and objectives of I.T. Act, 2000 is that it enables and facilitates the use of electronic commerce and also it provides equal treatment to the users of paper based documentation and to those who are signing computer based information.

This Act has the "Fundamental Equality Approach" and it doesn't differentiate between the paper and the paper-less documents. According to the law in this Act, any kind of document is admissible in the court of law. In digital, any kind of copy will be treated as original. This Act relates to the words such as "Writing", "Signature", "Original" of traditional paper-less world.

What is the Scope of I.T. Act, 2000?

The I.T. Act, 2000 has been enacted to facilitate "Electronic Commerce" and "E-Governance". A characteristic of E-commerce is that through the process of cryptography, the e-transactions will be secured. The cryptography protocol includes encryption, i.e., using private key for securing the message and decryption, i.e., using the public key to get the message from electronic signature. And also there is a participation of at least one trusted third party i.e., certifying authority to the transaction.

This Act also facilitates E-governance. It means for better government services provided to citizens, I.T methods should be used. For example, paying taxes using income-tax department websites, downloading various forms and checking results by visiting government websites, getting knowledge about government bye-laws, rules and regulations. This use of websites by citizens' help them to get time-to-time knowledge of amendments made in government rules and also help them to live better life.

The main criterion of Information Technology Act is that it is technology- intensive law. It accepts "Electronic signatures" as an authentication standard and it gives the identity of the sender and authenticates the contents. It also keeps the information personal and integrates and authenticates the information.

This Act also facilitates international trade and is helpful in paper-based communication and storage of information. The Act is not only related to UNCITRAL'S model of law on electronic commerce but it also relates to other aspects of Information Technology so that government should deliver services by its reliable electronic means.

United Nations Commission on International Trade Law (UNCITRAL) is a Model law on electronic commerce adopted by UN General Assembly on 30th January, 1997. This is also known as mother law.

It was held by Supreme Court in *Konkan Railway Corporation Ltd. v. Rani Construction Private Ltd.*, MANU/SC/0053/2002 : (2002) 2 SCC 388, it was held "That the UNCITRAL model law taken into account only for drafting of Arbitration and Conciliation Act, 1996 is patent from the Statement of Objects and Reasons of the Act. The Act and the model law are not identically drafted."

While enacting the Information Technology Act, 2000 the true intention of Legislature was that the Act must fulfil the national and municipal perspectives of information technology and other intention was that it must fulfil the international perspectives also.

What was the micro and macro perspective of United Nations?

United Nations had micro and macro perspectives in framing the international law.

The macro perspectives were:-

- 1.To facilitate e-commerce in various nature.
- 2.To validate transactions entered into by means of information technologies.
- 3.To promote various other information technologies.
- 4.To promote uniformity of law.
- 5.To support commercial practice.

The micro perspectives were:-

- 1.To establish rules and norms that validates and recognizes contracts, forms through electronic means.
- 2.To define the characteristics of valid electronic writing and an original document.
- 3.To provide acceptability and authenticate the electronic signatures for legal and commercial purposes.
- 4.To support the admission of computer evidence in courts and arbitration proceedings because whatever is created, it is acceptable in court of law.

Which countries join the digital signatures club membership?

There are various countries which join 'electronic signatures' club membership. India is the 12th country to join it. Other countries are:-

Australia, Canada, Denmark, France, Germany, Italy, Japan, Malaysia, Philippines, United Kingdom, United States, South Korea, Singapore and Sweden.

Extent of Information Technology Act, 2000

It shall extend to whole of India and includes State of Jammu and Kashmir, it also applies to other countries where the offences are committed by any person related to Information Technology.

Under article 253 of Indian Constitution, it states that "Notwithstanding anything in the foregoing provisions of this chapter, Parliament has power to make any law for the whole or any part of the territory of India for implementing any treaty, agreement, or convention with any other countries or any decision made at any international conference, association or other body."

Therefore, in view of this provision, this Act applies to the State of Jammu and Kashmir.

What is the Jurisdiction of I.T Act?

Write a Note on Applicability of I.T. Act, 2000?

This Act has extra-territorial jurisdiction. It applies to any offence or contravention committed outside India by any person, section 1(2) irrespective of his nationality, (section 75). The offence committed by person involves the computer, computer system or computer network located in India, and the offence is committed in India or outside India, but it is also necessary that the computer, computer system is located in India.

Certain Instructions/documents are non-applicable under the Information Technology Act. The questions of non-applicability of certain Instruments or documents are understood from their conversion into electronic records.

(a)The Information Technology Act is also non-applicable to the negotiable instrument which is defined under section 13 of the Negotiable Instruments Act, 1881. The reason of non-applicability was the lack of electronic funds transfer system in India and also there was no governing body to regulate it. But after the amendment of Negotiable Instruments Act, 2002, this Act is applicable because of electronic fund transfer system and other electronic Negotiable Instrument system through electronic medium has become easier.

The main object of the Information Technology Act was to facilitate e-commerce and to promote e-business. Therefore, the digital negotiable Instruments like e-cheque, e-cash came into existence after the enactment of this Act but lacked legal validity.

After the amendment of the Negotiable Instruments (Amendment and Miscellaneous Provision) Act, 2002, the definition of cheque is defined under section 6 as "A 'cheque' is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on demand and it includes the electronic image of a truncated cheque in the electronic form."

The words in section "electronic image" itself says that the "cheque" has gained the electronic value. It is applicable under Information Technology Act. The function of cheque under The Negotiable Instruments Act is equivalent to the electronic cheque.

(b)The Information Technology Act is non-applicable to the power of attorney which is defined under section 1A of the Power-of-Attorney Act, 1882.

Power-of-Attorney is executed on non-judicial stamp paper. It cannot be in electronic form because Power-of-Attorney is made on stamp paper only and stamp revenue goes to government and Stamp Act is not subject to changes. There is no stamp paper in electronic form.

(c)A trust defined in section 3 of the Indian Trusts Act, 1882 is also non-applicable to the Information Technology Act, 2000. A trust deed cannot be in electronic form. It is executed on non-judicial stamp paper and stamp duty directly goes to the Government. Stamp paper on which trust deed is made cannot be in electronic form.

Section 3 of the Indian Trust Act, 1882, defines trust as "an obligation annexed to the ownership of property,

and arising out of a confidence reposed in and accepted by the owner, or declared and accepted by him, for the benefit of another or of another and the owner."

(d) A Will is defined in clause (h) of section 2 of the Indian Secession Act, 1925. It is also not applicable to the Information Technology Act, 2000. It is defined as "The legal declaration of the intention of a testator with respect to his property which he desires to be carried into effect after his death."

The Will is not applicable to the Information Technology Act, 2000 because in order to have "Will" there should be two witnesses and the signature of the witnesses is the mandatory requirement. It is impossible to encrypt the document with three different electronic signatures. (They are not in mass circulation).

(e) Any contract for the sale or conveyance of immovable property or any interest in such property is also not applicable to the Information Technology Act, 2000.

Section 2(10) of the Indian Stamp Act, 1899 defines "A conveyance on sale and every instrument by which property, whether movable or immovable, is transferred and which is not otherwise specifically provided by Schedule I."

The registries of movable or immovable properties are not online. Registry is still accepting physical records. The Registrar cannot deal with the citizens and does not accept their documents through online medium. The documents must be handed over to the Registrar.

(f) The documents or the transactions which are notified by the Central Government in the Official Gazette are not applicable to the Information Technology Act, 2000.

Attribution, Acknowledgment and Dispatch of Electronic Records

Attribution of electronic record to the originator-Section 11 of the Information Technology Act, 2000 says that an electronic record is attributed to the originator if it was sent by originator or by person who has authority to act on behalf of the originator or by an information system programmed by or on behalf of the originator.

1. Acknowledgment of receipt - Section 12 of the Act says that an acknowledgment is given by addressee in a particular method that is by communication or by a conduct of the addressee which indicates to the originator that the electronic record has been received where the originator states that electronic record shall be binding only on receipt of the acknowledgment, then unless he does not receive the acknowledgment, it will be assumed that electronic record has never been sent by the originator.

2. Dispatch and receipt (section 13) - The dispatch of an electronic record occurs only when it enters a computer resource outside the control of the originator and the receipt of record occurs otherwise than as agreed between the parties as follows:

(a) If the addressee has designated a computer resource for the purpose of receiving electronic record-

❖ Receipt occurs at the time when the record enters the designated computer record, or

❖ When the record is sent to the computer record not designated by the addressee, receipt occurs at the time when the addressee retrieves the record.

(b) If the addressee has not designated the resource within timings, the receipt is deemed to occur when the electronic record enters the computer resource of the addressee.

The place of dispatch is deemed to be the place where the originator has his place of business and is deemed to receive where the addressee has his place of business.

What is secure digital signature?

The parties who have applied for electronic signature always ask for security and it must be agreed by the parties. It can be verified that an electronic signature at the time it was affixed was-

1. Unique to the subscriber affixing it.
2. Created under the exclusive control of the subscriber related to the electronic record to which it relates in such a manner that if the record was altered the electronic signature would be invalid.

Explain the appointment, function of the Controller of certifying.

Regulation of Certifying Authorities

The Central Government may appoint a Controller of Certifying Authority by notification in Official Gazette and also appoint Deputy Controllers, Assistant Controllers, other officers and employees as it deems (Section 17). The Deputy Controllers and Assistant Controllers perform the functions assigned to them by Controller. The functions, duties and Head office and Branch office of the Controller is to be decided by the Central Government.

Functions of Controller are:- (Section 18)

- (a) Exercising supervision over the activities of the Certifying Authorities.
- (b) Specifying the qualifications and experience of the employees and the conditions subject to which the Certifying Authority may perform its function.
- (c) Specifying the form and content of an electronic signature certificate and the manner in which accounts are to be maintained.
- (d) Specifying the terms and conditions for appointment of Auditors and the remuneration to be paid to them.
- (e) Resolving the disputes between the Certifying Authorities and the subscriber, laying down duties and facilitating the establishment of any electronic system.

Briefly describe the process of issuing, renewal, rejection, suspension of license of electronic signature certificates under the various provisions of law.

The person who is applying for electronic signature certificates must write an application to the Controller of Certifying Authority and must fulfil the requirement as prescribed by the Central Government. The license is valid only for the period prescribed by the Central Government. It is not transferable or heritable. (Section 21).

An application for issue of license shall be accompanied by - (Section 22)

- (a) A certification practice document.
- (b) A statement including the procedures with respect to identification of the applicant.
- (c) Payment of fees not exceeding 25,000 rupees.
- (d) Other documents as prescribed by the Central Government.

Renewal of license - (Section 23) An application for renewal of license shall be made within 45 days before the expiry of the period of the validity of license. It must be in proper manner and along with fees not exceeding 5,000 rupees.

Suspension of license - (Section 25) The Controller after making an enquiry and if he thinks that a Certifying Authority has-

- (a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;
- (b) failed to comply with the terms and conditions subject to which the license was granted;
- (c) failed to maintain the procedures and standards specified under section 30;
- (d) contravened any provisions of this Act, rule, regulation or order made thereunder; he may revoke the license.

The Controller must have reasonable ground to revoke the license. No license shall be suspended for a period exceeding 10 days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension. Once the license has been suspended the Certifying Authority shall not issue any electronic signature certificate. (Section 25)

The Controller must publish the notice that the license of the Certifying Authority is suspended or revoked. (Section 26)

The Controller or any officer authorized by him shall take up investigation of any contravention of the provision, rules or regulations made under this Act. (Section 28)

If the Controller has the reasonable cause to suspect that any contravention of the provision of Chapter 6 of the I.T. Act has been committed, have access to any computer system, any apparatus data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. (Section 29)

What is the procedure to be followed by certifying authority?

Section 30 of the Information Technology Act talks about the procedure followed by Certifying Authority and lays down that every Certifying Authority shall.

1. make use of hardware, software and procedures that are secure from misuse; [section 30(a)].
2. provide a reasonable level of reliability in its service which must be suited to the performance of intended function; [section 30(b)].
3. adhere to the security procedures to ensure that secrecy and privacy of the electronic signature are assured; [section 30(c)].
4. be the repository of all electronic signature certificates; [section 30(ca)].
5. publish information regarding its practices, electronic signature certificates and current status of such certificate; [section 30(cb)].
6. observe other standards prescribed by the regulation [Section 30(d)].

Disclosure - Section 34

Every Certifying Authority shall disclose-

1. Its electronic signature certificate.
2. Any certification practice statement.
3. Notice of revocation or suspension of its Certifying Authority certificate.
4. Any other fact or document which adversely affects the reliability of a electronic certificate or Authority's ability to perform its services.

How the Electronic Signature Certificate Is Issued? Section 36

A Certifying Authority shall certify that:

1. It has complied with the provisions and rules of this Act.
2. The digital signature certificate has been published and is made available to person who is relying on it and subscriber has accepted it.
3. The subscriber holds the private key corresponding to the public key, as listed in digital signature certificate.

- 4.The subscriber holds a private key which is capable of creating a digital signature.
- 5.The public key to be listed in the certificate can be used to verify a digital signature offered by the private key held by the subscriber.
- 6.The subscriber public key and private key constitute the functioning key pair.
- 7.The information contained in the digital signature certificate is correct and accurate.
- 8.It has no knowledge of material fact, which if included in digital signature certificate would affect the reliability of representation in clauses (a) to (d). (Section 36)

How the Digital Signature Certificate is suspended? Section 37

The certifying authority suspends the digital signature certificate on receipt of a request from:

- 1.The subscriber listed in the digital signature certificate.
- 2.Any person who is authorized on behalf of the subscriber.

The certifying authority may also suspend the certificate in public interest.

Suspensions shall not exceed the period of fifteen days unless the subscriber has been given the opportunity of being heard.

Revocation - Section 38

A Certifying Authority may revoke the digital signature certificate issued by it after giving opportunity of being heard to the subscriber and if revoked, then communicate it to the subscriber on the following conditions:

- 1.Where the subscriber or any other person authorized by him to make a request.
- 2.Upon the death of subscriber.
- 3.Upon the dissolution of firm or winding-up of the company where the subscriber is firm or company.
- 4.Where the material fact is represented in the digital signature certificate is false or has been concealed.
- 5.Where the requirement of issuance of digital signature certificate is not satisfied.
6. Where the Certifying Authority's private key or security system was affecting the reliability of the digital signature certificate.
- 7.Where the subscriber has been declared insolvent or dead.

What are the various duties of subscribers?

Duties of Subscribers

- 1.Section 40 - Generation of key pair by subscriber by applying the security procedure.
- 2.Section 41(1) - Acceptance of digital signature certificate - A digital signature certificate is accepted by the subscriber when he publishes or authorizes the publication - (a) to one or more persons, (b) in a repository, (c) demonstrates the approval of digital signature certificate in any manner.
- 3.Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in the digital signature certificate and take all necessary steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber. It is the duty of the subscriber to communicate the compromise relating to private key corresponding to the public key, without any delay to the Certifying Authority, it is also declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

4. Section 41(2) - After accepting the digital signature certificate, all representations and information contained in that shall be held true for the purpose of relying on the information available in the digital signature certificate. The subscriber shall also hold the private key corresponding to the public key listed in digital signature certificate. The subscriber must also have all relevant information relating to the certificate.

Penalties and Compensation for Damage to Computer, Computer System etc. - Section 43

If any person without the permission of owner or any other person who is in charge of a computer, computer system or computer network-

1. Accesses such computer, computer system or computer network or computer resource.
2. Downloads copies or extracts any data, computer database or information.
3. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
4. Damages or causes to be damaged any computer, computer system or network data, computer database or any other programmes.
5. Disrupts or causes disruption.
6. Denies or causes the denial of access to any person authorised to access.
7. Provides any assistance to any person to facilitate access in contravention in provisions of this Act.
8. 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.
9. Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.
10. Steals, conceals, destroys or alters any computer source code with an intention to cause damage.

Then that person shall be liable to pay damages to the person affected.

General Definitions - Section 43

1. "Computer contaminant" means any set of computer instructions that are designed-
 - (a) To modify, destroy, record, transfer data or programme residing within a computer system or computer network.
 - (b) By any means to usurp the normal operation of the computer, computer system or network.
 - (c) "Computer Database" means representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared in a formalised manner or have been produced by a computer, computer system or network.
2. "Computer Virus" means any computer instruction, information data or programme that destroys, damages, degrades or adversely affects the performance of computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed.
3. "Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
4. "Computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Penalty for Failure to Furnish Information, Return, etc. - Section 44

If any person who is required to-

1. Furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, then he has to pay penalty not exceeding one lakh and fifty thousand rupees for each such failure.
2. File any return or furnish any information, books or other documents within the time specified, he shall be liable to pay penalty not exceeding five thousand rupees for every day during which such failure continues.
3. Maintain books of accounts or records, fails to maintain the same then he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Residuary Penalty - Section 45

If any person contravenes any rules or regulations made under this Act, then he shall be liable to pay a compensation of twenty-five thousand rupees to the person affected after such contravention.

Power to Adjudicate - Section 46

1. The Central Government shall appoint any officer not below the rank of a Director to the Government to be an adjudicating officer for holding an enquiry for any contravention of any of the provisions of this Act or any rule, regulation, direction, or any order made under the Act.
2. A reasonable opportunity for making a representation shall be given to the person against whom the enquiry was made by the adjudicating officer, and on his satisfaction, he may impose such penalty or award such compensation as he deems fit. The jurisdiction of adjudicating officer shall be specified by the Central Government.
3. The adjudicating officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore. In cases of claim for injury or damage exceeding rupees five crore the jurisdiction shall vest with the competent court.
4. Factors to be taken into account by the adjudicating officer -

(Section 47)-

- (a) The amount of gain of unfair advantage wherever quantifiable made as a result of the default.
- (b) The amount of loss caused to any person as a result of the default.
- (c) The repetitive nature of the default.

The Cyber Appellate Tribunal

Sections 48 to 64 deals with the Cyber Appellate Tribunal.

Section 48 - The Central Government shall establish one or more appellate tribunals and places in which the tribunal may exercise its jurisdiction.

Section 49 - The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other members, as the Central Government may, by notification in Official Gazette, appoint. The selection of Chairperson and other members of Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

Section 50 - A person shall not be qualified for appointment as a Chairperson of the Tribunal unless he is or has been or is qualified to be a Judge of the High Court.

The members of Cyber Appellate Tribunal shall be appointed by the Central Government, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.

Section 51 - The Chairperson or member shall hold office for a term of five years from the date on which he enters the office until he attains the age of sixty-five years and shall not be removed from the office except by an order by the Central Government on the ground of proved misbehaviour in court.

Section 52A - The Chairperson of the Cyber Appellate Tribunal shall have the power of superintendence and directions in the conduct of the affairs of that Tribunal.

Section 52C - The Chairperson of the Cyber Appellate Tribunal have power to transfer any case pending before one Bench to other Bench for disposal.

Section 52D - If the opinion of the members of a Bench differs, then they can make references to the Chairperson of Cyber Appellate Tribunal who hears to the point himself and decides the point according to the majority of members who have heard the case, including those who first heard it.

Procedure and Powers of the Cyber Appellate Tribunal (Section 58)

(1)The Cyber Appellate Tribunal shall be bound by the procedure laid down by the Code of Civil Procedure, 1908 and guided by the principles of natural justice, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place in which it has its sittings.

(2)The Cyber Appellate Tribunal, for the purpose of discharging their function, while trying a suit, in following matters, namely-

- (a)summoning and enforcing the attendance of any person and examining him on oath,
- (b)requiring the discovery and production of documents or other electronic records,
- (c)receiving evidence on affidavits,
- (d)issuing commissions for the examination of witnesses or documents,
- (e)reviewing its decisions,
- (f)dismissing an application for defaults or deciding it ex parte,
- (g)any other matter which may be prescribed.

Section 59 - The appellant may appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

Section 60 - Limitation.-The Provisions of Limitation Act, 1963 apply to an appeal made to Cyber Appellate Tribunal.

© Universal law Publishing Co.

CHAPTER VII

Cyber Crime

Synopsis

7.1 Introduction

7.2 Other Computers-related Offences

7.3 I.T. Critical Infrastructure in India

Protected System

Privacy in Indian Context

Another Leading Case on "Right to Privacy"

7.4 Classification of Offences against Other Laws

7.5 Classification of Cyber Offences

Penalty for Damage to Computer, Computer System, etc. Section 43

7.1 Introduction

There are two groups of crimes. One group is computer crimes where crime is committed by the computer or a tool used to commit crime is a computer. Other group is computer related crime where computer can be used in evidence.

What is computer crime?

Computer crime is done against an individual or an organization where perpetrator of a crime uses a computer or computer technology to commit crime. Computer related crimes are hacking, creation of virus, credit cards theft, electronic fund transfer fraud, etc. These are the crimes in which computer acts as a necessary tool. But computer acts as an evidence of crime which are not related to computer but where information is taken about a registered code then it is easy to prove the case.

66. Computer related offences.-

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

Explanation.-For the purposes of this section,-

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

66A. Punishment for sending offensive messages through communication service, etc.-

Any person who sends, by means of a computer resource or a communication device,-

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

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.-For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66B. Punishment for dishonestly receiving stolen computer resource or communication device.-

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

66C. Punishment for identity theft.-

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

66D. Punishment for cheating by personation by using computer resource.-

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

66E. Punishment for violation of privacy.-

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

Explanation.-For the purposes of this section-

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that;-

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism.-

(1) Whoever,-

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

or any section of the people by-

- (i) denying or cause the denial of access to any person authorized to access computer resource; or
- (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
- (iii) introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70 or

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

commits the offence of cyber terrorism.

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

2. Source code alteration - Section 65 - It means that if any person conceals, destroys or alters the computer source code which includes computer programs, computer commands, designs, computer network, when this source code is required to be mentioned by law then the person is said to be punished for tampering with the computer source document. Therefore, it is necessary that every organization should register its security code. Sometimes, it is difficult for an organization that the security code is their property or not. So, if they have the code, the person falling under this section is entitled to be punished for imprisonment of three years or fine of Rs. two lakh or both.

Crimes of alteration of computer data are:-

- i. False Data Entry
- ii. Data Leakage
- iii. Virus
- iv. Worms
- v. Trap Doors
- vi. Computer Forgery
- vii. Program Piracy
- viii. Fraud at Payment Points
- ix. Program Manipulation
- x. Software Piracy.

3. Punishment for publishing or transmitting obscene material in electronic form (Section 67)

If any person publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who

can read, see or hear the matter contained in it, shall be punished for the term of 3 years or with fine of Rs. five lakhs and in the event of second or subsequent conviction the imprisonment will be for the term of 5 years and also with fine which may extend to Rs. ten lakhs or both.

(Section 67A) - This section is related to the publishing or transmitting of material containing sexually explicit act, etc., in electronic form. This conduct shall be punished on first conviction with imprisonment for five years and fine of ten lakhs rupees and in second conviction imprisonment of seven years and also with fine which may extend to ten lakh rupees.

This section includes the person who:

- (a) publishes or transmits any material in electronic form which depicts children engaged in sexually explicit act or conduct; or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges, distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
- (c) cultivates or induces children to online relationship with one or more children for and on sexually explicit act or in a matter that may offend a reasonable adult on the computer resource; or
- (d) facilitates abusing children online; or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

4. Other Computer related offences (section 66). If any person does any act as referred to in section 43 of the Indian Penal Code, then he shall be punished with imprisonment of two to three years or with fine of Rs. five lakhs or with both.

Other Offences are:

(Section 66A) - Punishment for sending offensive messages through communication services, etc. It means if any person sends any offensive message which is grossly offensive or has menacing character or if he knows it to be false or causing inconvenience, insult, injury, criminal intimidation, enmity, hatred or ill will then the punishment will be for three years or with fine or both.

(Section 66B) - This section relates to receiving or retains any stolen computer resource or communication device, and the person knows or believes that it has been stolen, then he shall be punished with imprisonment of three years or with fine of one lakh rupees or both.

(Section 66C) - Punishment for identity theft if any person fraudulently make use of the electronic signature, password or other identification feature of any other person, then he shall be punished with imprisonment of three years and also liable to fine of rupees one lakh.

(Section 66D) - If any communication device or computer resource cheats by personation, then the person shall be punished with imprisonment of three years and also liable to fine of one lakh rupees.

(Section 66E) - If a person intentionally captures, publishes, transmits the image of a private person and violates his privacy then he shall be punished with imprisonment of three years or with fine not exceeding two lakh rupees or both.

(Section 66F) - Cyber Terrorism is a crime in which a person

(A) with intent to threaten the unity, integrity, security or sovereignty of India or strike terror in the people by-

- (i) denying or cause the denial of access to any person authorized to access computer resource; or
- (ii) attempting to penetrate or access a computer resource without authorization; or

(iii) introducing any computer contaminant and such conduct likely to cause death or injury to persons or damage or destruction of property or services which are essential to the life of community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally accesses a computer resource without authorisation and by means of such conduct obtains access to information data or computer database that is restricted for security of State or foreign relations and it is believed that such information, data causes injury to the sovereignty and integrity of India, the security of the State, public order, decency, morality, or in relation to contempt of court, defamation, or to advantage of any foreign nation or group of individuals commits the offence of cyber terrorism. The person shall be punished with imprisonment for life.

The other provisions of the law which are related to this section are the Indecent Representation of Women Prohibition Act and section 292 of the Indian Penal Code.

Section 292 of the Indian Penal Code is related to obscenity in physical paper material. Therefore, section 67 of I.T. Act, 2000 is a comprehensive section. This section catches the violators of law and punishes them. It is a wide section which is not restricted to only indecent representation of women.

To provide evidence to the court, it is purely upon discretion of court, whether to take the evidence as an important evidence or not. If a person is in a position to give an evidence to prove his case, then he should certify for operating of the computer. The reliability of the evidence will not be reduced in any circumstances and it is difficult for hacker to prosecute and convict himself by altering or destroying programmes as data stored in a computer system.

☞ Landmark judgment on section 67 held that if any abusive matter is contained in a book then it is necessary to find out that whether it is obscene or not and whether it deprave and corrupt the mind of persons to the extent which are open to influences of this sort; *Ranjit D. Udeshi v. State of Maharashtra*, (1965) 1 SCR 6556: MANU/SC/0080/1964 : AIR 1965 SC 881.

☞ *Samaresh Bose v. Amal Mitra*, AIR 1986 SC 967: 1986 Cr LJ 24.

In this case, the Judges expressed their view that "In our opinion, in judging the question of obscenity, the judge in the first place should try to place himself in the position of author and from the point of view of the author the judge should try to understand that what is it that the author seeks to convey and what the author conveys has any literary and artistic value. The judge thereafter should place himself in the position of a reader of every age group in whose hand the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers. The judge should thereafter apply his judicial mind dispassionately to decide whether the book in question can be said to be obscene within the meaning of the section by an objective assessment of the book as a whole and also the passage complained of as obscene separately".

In other leading case, in which test of obscenity is done is *Miler v. California*, 413 US 15 is also called the 'Miler Test':-

(1) Whether "the average person", applying for community standard, would find the work appealing to the prurient interest.

Here community standards in different places are different, e.g., in California, in case of modern times, the orthodox standards have to be seen.

(2) Whether the work depicts or describes in a patently offensive way, sexual conduct specifically defined by State law.

(3) Whether the work lacks serious literary, artistic, political or scientific value.

(4) Whether the work so made is obscene or corrupts the minds of persons.

If the above mentioned questions are satisfied or if the above test is done, then it will be proved that the matter in question is obscene or not. To prove that the matter is obscene it is mandatory to do the above test and satisfy the above question.

7.2 Other Computer-related Offences

(1) In the leading metropolitan case of PANCARDS, an individual was forging PANCARDS to be used as identity proof. Offender forged more and more PANCARDS for those people who were paying him more advance with fictitious address to claim the refund.

(2) Computer Virus:- It is a program which is spread to whole of computer system, attaching copies itself to ordinary programs. The latest case that took place on Feb 3, 2006 was the Kama Sutra Virus. Many countries networks were affected due to this virus.

"Kama Sutra" is a mass mailing worm that attempts to lower your security settings and disable anti-virus software. It arrives in your mail box, pretending to be from someone you know, with a variety of subject lines, including: "My Photos", "Funny", "A Great Video", "Hot Movie" and others. Once activated, on the 3rd day of each month, the worm begins overwriting Word and Excel documents, as well as .zip, .pdf, and others, and thus destroying their contents. In some instances, an infected computer may have the addition of the tray icon "Update Please wait" in the lower right hand corner of your screen. Kama Sutra has been rated a "low" risk by McAfee.com but may be upgraded soon due to the escalating rate of infection.

(3) Black Mail:- Now-a-days, people are blackmailing each other by putting up a message which contains virus in the other person's system. The virus are also sent through mobile phones in order to destroy them.

(4) Pornography:- It is easily seen on internet as it gives the whole situation of the depravity of the society. It is duty of internet services provider to prevent the use of these services to distribute pornographic material and remove it whenever it is detected.

Example:- The Delhi Public School case of MMS was the famous case in which the school boy and school girl having sex were caught up by a camera phone. Mass mailing was held with a speed and on line sale also took place. The same was also put on line at Bazee.com by a student of IIT, Kanpur. It was the case of pornography in which an alarming situation of society was available on internet.

(5) Threatening e-mails:- There are many cases of threatening e-mails with the growing and powerful instrument. It is affecting the personal life of individuals and also disturbing the social environment as a whole. Recently, a person had sent a threatening e-mail from

Tamil Nadu to Parliament mentioning that there was a bomb placed in Parliament premises.

(6) Telecommunication Fraud:- It is also increasing day-by-day. Information of telephone calls which is stored on a computer that is linked to a telecommunications system is valuable. The world of telecommunications is giving rise to many crimes. A new era of wireless devices has also come up. Crimes related to telecommunications are non-payment of call once the service is activated, an unsigned number is provided to the user that does not have an account with the network, etc.

(7) Identity Theft:- Financial frauds are committed with the help of this crime. If the hacker comes to know about the credit card details or other bank account details of the victim then he can place himself in the place of victim and perform all fraudulent activities like transferring of money in his account.

(8) Conspiracy to defraud:- Under this fraud, two or more persons operate a computer by passing a password which they should not do. They do this act to transfer the funds in their own account. They have the intention to commit crime and this act is committed by two or more than two persons, so, at the time of trial, they all will be tried as they all are liable for this act.

(9) Alteration of Input Data:- It is a situation where data stored in the computer is altered in order to use it again or

sell it, with an intention to commit crime. The data which is so altered is without the permission of data holder.

7.3 I.T. Critical Infrastructure in India

Protected System

Section 70-Section 70 of I.T. Act, 2000 states that the appropriate government may declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure to be a protected system. Only authorised persons can have access to the protected system. Any person who secures access or attempts to secure access to a protected system in contravention of the provision, then he shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

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

Section 70 of I.T. Act, 2000 has the deterrent effect over and above section 66 of the Act. For example:-Railway Reservation network is declared as a protected system under section 70 of this Act. Then if some one hacks into such Railway Reservation network then he would get an imprisonment upto ten years. But suppose if Railway Reservation network is not protected under section 70 of the I.T. Act, 2000 wherein he may get imprisonment upto three years. It is thus important that in order to protect IT infrastructure related to national security, operational networks like income-tax department, airport authority, railways, etc., should be declared as "Protected System" under section 70 of I.T. Act, 2000 by the appropriate government by notification in Official Gazette. The hacker of same will also be tried under section 70 of the I.T. Act, 2000 and will be punished accordingly.

National Nodal Agency

Section 70A of the I.T. Act provides that the Central Government may designate any organisation of the Government or the National Nodal Agency which will be responsible for all measures including research and development relating to protection of the Critical Information Infrastructure.

Indian Computer Emergency Response Team

What is the Indian Computer Emergency Response Team? What are its function. What is the punishment for failure to comply with the directions of the Computer Emergency Response Team?

Section 70B of the I.T. Act lays down that the Central Government shall appoint an agency of the Government to be called the Computer Emergency Response Team. The team shall serve as the notional agency for performing the following function in the area of cyber security:-

- (a)collection, analysis and dissemination of information on cyber incidents;
- (b)forecast and alerts of cyber security incidents;
- (c)emergency measures for handling cyber security incidents;
- (d)coordination of cyber incidents response activities;
- (e)issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- (f)other functions relating to cyber security.

The Indian Computer Emergency Response Team may call for information and give direction to the service providers, intermediaries, data centres, corporate body and any other person. If any such service providers, intermediaries fail to provide the information called for or fails to comply with the directions, shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

Section 72 of I.T. Act, 2000 states that any person who, in pursuance of any of the power conferred under the I.T. Act, has secured access to any electronic record, book, register, correspondence, information, document, or any

other material without the consent of any other person or discloses it to any other person then he will be punished with imprisonment upto two years or fine of one lakh rupees or both.

Under this section, it is also mentioned that "any person who, in pursuance of any of the power conferred". Therefore, limited persons who are empowered under this Act are Controller of Certifying Authority, its staff, Presiding Official, police officers and network service providers. Scope of section 72 is limited to these persons only. Power and functions of Controller are mentioned under section 18 of I.T. Act, 2000 in detail.

What is the penalty for Breach of Confidentiality and Privacy?

Privacy in Indian Context

Right to privacy is provided as a Fundamental Right under article 21 of the Constitution of India which states that "no person shall be deprived of his life or personal liberty except according to procedures established by law".

The first case where for the first time Hon'ble Supreme Court introduced the Right to Privacy under article 21.

Kharak Singh v. State of Uttar Pradesh, MANU/SC/0085/1962 : AIR 1963 SC 1295: 1963 (2) Cr LJ 329.

Appellant was harassed and tortured by police under regulation 236(b) of Uttar Pradesh Police Regulation which permits the right of domiciliary visits at night to the appellant. But in this case, appellant's right was taken away by police and he was not allowed for domiciliary rights at night.

It was held that regulation 236 is unconstitutional and in violation of the article 21 of the Constitution of India. Judge ruled that article 21 of the Constitution to include "right to privacy" as a part of the right to "protection of life and personal liberty".

In R. Rajagopal v. State of Tamil Nadu, MANU/SC/0056/1995 : (1994) 6 SCC 632: AIR 1995 SC 264.

It was held that the right of privacy includes the right to life and life guaranteed to the citizen by article 21. Every citizen has right to safeguard the privacy of his family, marriage, motherhood, childbearing, education and himself. No other person has a right to interfere with the right of other person. In the above case, for the first time, Court has winded the concept of "right to privacy".

In India, we do not have any specific data protection or a legislation dealing with privacy of an individual. Therefore, the courts used article 21 to interpret privacy rights guaranteed to citizens by our Indian Constitution.

Explain the concept of right to privacy along with leading cases?

Another Leading Case on "Right to Privacy"

PUCL v. Union of India, MANU/SC/0149/1997 : (1997) 1 SCC 301: AIR 1997 SC 568.

Facts of the case: PUCL filed a case under article 32 against the incidents of telephone tapping of political persons. The issue had constitutional validity of section 5(2) of the Indian Telegraph Act, 1885 in light of article 21 and article 19(1)(a) of the Constitution of India. Section 7 of the Indian Telegraph Act, 1885 talks about framing of procedure guidelines for the effective use of section 5(2), this Act came into force in 1885 which deals with phone tapping and it is regulated by Secretary, Ministry of Home Affairs. It was held in this case that right to privacy is a part of "right to life and personal liberty" which is mentioned under article 21 of the Constitution. No other person has a right to curtail this right except according to procedure established by law. Therefore, in this case, right to have telephonic conversation in the privacy of ones home or office without any interference comes under "right to privacy". No other person has a right to listen or interfere in the telephonic conversation of any person. Hence, telephonic conversation does not come under article 21 of the Constitution of India unless it is permitted under the procedure established by law. Also, when a person is talking on phone, he is expressing his views and he has a right to freedom of speech and expression, enumerated under article 19(1)(a) of the Constitution.

☞ Under this Act Cr. P.C., Schedule I, Part II is also followed.

☞ Under the First schedule, classification of offences is done.

☞ These are the offences under the Indian Penal Code.

7.4 Classification of Offences Against Other Laws

☞ Cognizable offences are those for which a police officer may arrest without a warrant.

☞ Non-cognizable offences are those for which a police officer shall not arrest without warrant.

If for a particular offence, a person is punished with death, imprisonment for life or imprisonment for more than seven years then it will be cognizable offence and it will be triable by Court of Session.

If for a particular offence, person is punished with imprisonment for three years and upward but less than seven years, then it will also be cognizable and non-bailable offence and it will be triable by Magistrate of First Class.

Therefore, if for a particular offence, a person is punished with imprisonment for less than three years and with fine only, then it will be non-cognizable and bailable offence and it will be triable by any Magistrate.

7.5 Classification of Cyber Offences

Section 65	Tampering with computer source document	Cognizable/Non-bailable
Section 66	Computer related offences	Cognizable/Non-bailable
Section 67	Publishing of obscene information in electronic form	Cognizable/Non-bailable
Section 70	Protected System	Cognizable/Non-bailable
Section 72	Breach of confidentiality and privacy	Cognizable/Non-bailable

Penalty and Compensation for Damage to Computer, Computer System, etc. Section 43

Section 43 of the I.T. Act provides that 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, computer network or computer source;

(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 authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

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

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or effects it injuriously by any means;

(j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

he shall be liable to pay damages by way of compensation to the person so affected.

'Access' means giving entry into instructing or communicating the logical, arithmetical or memory function resource of a computer, computer system, computer network. Damage to the computer also includes downloading of data, copying or extracting any data, computer data base or information from such computer, computer system, computer network including the data which is stored. Irremovable sabotage medium computer database is also explained under this Act. It means representation of information, knowledge, facts, concept, instructions in image, audio, video which are prepared in a formalised manner or have been produced by a computer, computer system, computer network. If any person has introduced or put up any virus or computer contaminant, then he will be punishable under section 43.

Damage to computer also includes disruption of any computer, computer system or computer network, the denial of access to any person authorised to access any computer, computer system or computer network by any means, provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention to provisions of this Act, 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. It also includes destroying, deleting or altering any information stored in computer system and diminishes its value and affects injuriously, steals, conceals, destroys or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

The person doing the above mentioned act shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Computer contaminant, is also defined under section 43 of this Act. It means any set of computer instructions that are designed to modify, destroy, record, transmit data or programming residing within a computer, computer system or computer network.

Computer virus means any computer data, instructions or information which degrades, damages, or destroys and affects the working or performance of the computer. Even this virus operates in such a manner that it can take place in a computer when it is attached to another computer resource and starts programming.

This section also covers the persons who are not the owners of the computer resource or they do not have the permission to use the computer system and they cause damage or destroy the computer, computer system, computer network, data, computer base. Damage by these persons include destroying, deleting, adding, modifying, or rearranging of any means.

If he disrupts or causes any disruption of any computer, computer system, computer network or if he denies to any other person authorized to access any computer, computer system, computer network by any means, then also he will be covered under this Act.

The person can also provide any kind of assistance to any person to facilitate access to a computer, computer system, computer network in contravention of the provision of this Act, rules and regulations made thereunder and if he charged the services availing the person to the account of another person by tampering with or manipulating any computer, computer system, computer network,.

Then in all of the above circumstances, person will be covered under section 43 of I.T. Act, 2000 and he has to pay the damages by way of compensation to the person so affected.

(Section 43A) - Compensation for failure to protect data - Where a corporate body handling any sensitive data or information in a computer, computer resource which it owns, controls or operates, is negligent in maintaining reasonable security practices and procedures and causes loss, damage and wrongful gain to any person, then such

corporate body shall be liable to pay damages by way of compensation to the person so affected.

© Universal law Publishing Co.

Chapter VIII

Data Security and Data Protection

Synopsis

Issue of Confidentiality

Meaning of Confidential Information

Confidential Materials

Before going into detailed explanation of Data security and protection, it is necessary to define 'Data'. The term "Data" has been defined under Information Technology Act, 2000 under section 2(1)(o) as:-

- 1.Data means representation of knowledge, facts, concept or instructions.
- 2.Which are being prepared in a formalised manner.
- 3.And is intended to be processed, is being processed or has been processed.
- 4.In a computer system or computer network or may be in any form.
- 5.Or stored internally in the memory of computer.

Define computer Data Base?

Computer Data Base is defined under section 43 of I.T. Act, 2000. The ingredients of the section are:-

- 1.Representation of Information, knowledge, facts, concepts.
- 2.In a text, audio, video, image.
- 3.Those are being prepared or have been prepared.
- 4.In a formalised manner.
- 5.Or have been produced by a computer, computer system or computer network.
- 6.Intended for use in computer, computer system, computer network.

Data bases are created by two process, i.e.,

- 1.It is created by programming tools, e.g., Microsoft Outlook.
- 2.It is created by automated process(es).

Computer database are protected under I.T. Act. They are protected due to various reasons:

- 1.It is commercially valuable.
- 2.It is a product in which there is an investment of time, intellectual capital and money.
- 3.It is convenient to use.

Write a note on UK's Data Protection Act, 1998. Explain its purpose also.

UK's Data Protection Act, 1998.

It is built around eight data protection principles that apply to all personal data. It is also processed by data controllers including companies, business organizations, employers, local and Central Governments.

Data controllers also determine the purpose for which the personal data is processed and they also explain the manner and procedure in which personal data is processed.

UK's Data Protection Act applies to all personal data. Therefore, it is necessary to understand what is Personal Data.

Personal Data is nothing but a Data that relates to a living individual. That individual can be:-

- ❧• Identified from the Data.
- ❧• Other information which is in possession or likely to come into possession of data controller.
- ❧• Any expression of opinion, view about the individual.

There is also a sensitive personal Data. This type of Data is sensitive in nature and it cannot be shared with everyone. In India, there is no such Data Base Protection Act which defines personal or sensitive personal Data. Sensitive personal data includes:-

- (a)Racial and ethnical origin - Which some individuals want/desire to keep it personal.
- (b)Political opinions - Political opinions by various political thinkers and answers to the questions by general public are confidential if data controller desires so. If political news, opinions are disclosed in computer then it may result in rivalry or corruption or any bad evil.
- (c)Religious belief or other beliefs of similar nature - Various religious institutions keep their customs, ritual and their beliefs confidential in nature.
- (d)Membership of a trade union - Also confidential or sensitive in nature if data controller desires so.
- (e)Physical or mental health condition - Physical or mental health condition of an individual, or group of company or association need not be disclosed in computer. It is a sensitive issue and if data controller does not want to disclose this information, he can keep it confidential in nature.
- (f)Sex life of an individual is also a sensitive personal data.
- (g)Criminal offences - The offences which are criminal in nature, cannot be disclosed on computer because it may affect the human mind and corrupt it.
- (h)Criminal proceeding and convictions are also a part of personal data in which data controller does not disclose the data to general public.

The Eight Principles of Personal Data are:-

Personal Data:

- 1.Shall be processed lawfully and fairly.
- 2.Must be accurate and kept up to date.
- 3.Must be held only for lawful purposes which are described in registered entry.
- 4.Must be relevant and not excessive in relation to the purpose for which they are held.
- 5.Must be accessible to individuals who were to correct it, or erase it.
- 6.Must be protected by proper security.
- 7.Must be used or disclosed only for lawful or compatible purposes.
- 8.Must be there only for purpose for which they are held.

Issue of Confidentiality

What is the conceptual basis of confidentiality?

Parties to confidentiality agreements are:-

1. Disclosing party.

2. Receiving party.

In confidentiality agreement, there must be an express or implied term in a contract which imposes an obligation of confidence on both or either party. The person who has received any information in confidence shall not take unfair advantage of it. He must not make use of it to prejudice the person who gave it without obtaining the consent of that person.

Information becomes confidential only when its content needs to be protected or hidden from others. It needs protection merely because it is sensitive. If there is disclosure of information, it must be prevented from breach of an obligation to keep the information confidential.

Explain the main elements of confidence?

The elements of confidence are:-

1. Quality of confidence - The information which is sensitive and which needs protection must have the necessary quality of confidence.
2. Communication - The information must be communicated by one person to another and must have been communicated in circumstances imparting an obligation of confidence.
3. Unauthorized use of information - An unauthorized use of information which is detriment of party communicating it.

Define what is the "confidential information".

The confidential information is sensitive in nature. It needs protection by the person who knows the confidential information. The information must be such, the release of which the owner believes would be injurious to him or his rivals or others. The information is injurious that is the only reason why the owner wants it to be protected and keep it confidential. The owner believes that the information is confidential in nature and it is not in public domain.

The information becomes information only when it is deliberately disclosed by one party that is known as disclosing party to another receiving party. The obligations of confidence arise in an express or implied term of a contract. Disclosing party request the receiving party to keep the information confidential or secret. Sometimes, the nature of dealing between two parties show that the information should be kept confidential. Their terms and conditions show that the information related to business transaction must be kept confidential.

Meaning of Confidential Information

Any information, unauthorised disclosure of which could cause serious damage to the interest or cause serious embarrassment to the parties concerned or could effect functioning of an organisation.

Define what are confidential materials.

Confidential Materials

Confidential materials mean all tangible materials. Tangible materials are those which cannot be seen by naked eye and which can only be felt and can be in possession of one person. It includes confidential information which includes written or printed documents, computer disks, CDs, tapes, whether machine or user readable.

What material is not included in confidential materials?

A confidential material does not include any information that:-

1. Is publicly available without breach of any obligation owed to disclosing party by the receiving party.
2. There has been no disclosure by disclosing party to any one but the information has been known to the

receiving party prior to it became public.

3. The receiving party got the information from any other source other than disclosing party. There has been no breach of an obligation of confidentiality owed to the disclosing party.

4. The information has been developed by receiving party himself and not become known from any other source or disclosing party.

What kind of restrictions are there on the receiving party to keep the information confidential?

The receiving party shall not disclose any information to third parties following the date of its disclosure by disclosing party to the receiving party.

Explain the rights and remedies available with receiving party?

Receiving party also should take reasonable security to protect the confidential information and keep the information confidential. It is the duty of receiving party not to disclose information to any one. The receiving party can only disclose the information to the receiving party's employees, consultants on a need to know basis or on circumstantial basis. Whenever the need arises to know any information about business, product to the employees, then it is the duty of receiving party to disclose the information to employees because the receiving party has executed or shall execute written agreements with its employees and consultants sufficient to enable it to comply with all provisions of agreement.

After disclosing the confidential information by receiving party to its employees or consultants, the receiving party should immediately on disclosure of confidential information or confidential materials or any other breach of obligation agreement by receiving party, should notify the disclosing party. Receiving party should also co-operate with the disclosing party to regain possession of confidential information or confidential materials and should try best in every possible manner to protect the confidential information. It is the only right of receiving party.

When it is notified to disclosing party that receiving party has disclosed all confidential information to the employees, consultants, etc., then receiving party shall return all original documents, copies, CDs, tapes, records, reproductions, summaries of confidential information or confidential materials at disclosing party request and all materials will be destroyed by them at their option.

All confidential information and confidential materials remain the property of disclosing party. When the confidential information is disclosed by disclosing party to the receiving party, the disclosing party do not grant any express or implied right to receiving party, or under patents, trademarks, copyrights or trade secret information.

When disclosing party and receiving party come into an agreement that they will keep the information confidential or secret and will not export or import the confidential information or any product or service that is the part of confidential information and do not utilize them in design, development or production of nuclear chemical or biological weapons.

© Universal law Publishing Co.

CHAPTER IX

Introduction to Satellite, Media, Cable TV, Broadcast

Synopsis

Prasar Bharti (Broadcasting Corporation of India) Act, 1990

Section 2(a)-"Akashvani"

Section 2(c)-"Broadcasting"

Section 2(h)-"Doordarshan"

Section 3-The Prasar Bharti Board

Section 12-Functions and Powers of Corporation

Section 13-Parliamentary Committee

Section 14-Establishment of Broadcasting Council

Section 23-Powers of Central Government

Sections 32 and 33 Talk About the Rules of Corporation

Cable Television Networks (Regulation) Act, 1995

Section 2(a)-"Cable Operator"

Section 2(b)-"Cable Service"

Section 2(c)-"Cable Television Network"

Section 4-Registration as a Cable Operator

An Overview of the Telecom Regulatory Authority of India (Amendment)

Act, 2000

Section 14-Establishment of an Appellate Tribunal

Section 14N-Transfer of Appeals

Media is becoming more and more comprehensive nowadays. The term media was evolved in 1990's. Media makes a fine line between nationality, morality, personal rights and privileges like right to freedom, right to expression, etc. These rights come into existence only with the help of media. Article 19(1)(a) of the Constitution secures to every citizen of India, the freedom of speech and expression. This right means the right to express one's ideas and opinions. Lawmakers can only interfere with media in case of policy licensing and limiting the content.

Broadcasting began in 1926 with the setting up of a broadcasting company. The Government took over this company and named it as All India Radio in 1931. It became famous to give speech. The term "broadcasting" means the transmission by wireless means for public reception of sounds or of images and sounds. And "re-broadcasting" means transmission by one organization to another organisation. Example of re-broadcasting is, match shown on DD, Ten Sports channel. The Event remains same and signals also remain same. The transmission of encrypted signals is called as broadcasting where decrypting is provided to public by broadcasting organization. The television providers receive direct broadcast from the broadcasting organization which means it is relying on signals from the satellite.

THE PRASAR BHARTI (BROADCASTING CORPORATION OF INDIA) ACT, 1990

Broadcasting in India comes under the Prasar Bharati (Broadcasting Corporation of India) Bill which was introduced in

1979. Later, it became Prasar Bharti Act, 1990. Prasar Bharti means creating a governmental control over media, satellite channels with reference to contents and channels. The main purpose of this Act is to provide benefit to society.

The main definitions under the Act are:

Section 2(a)-"Akashvani"

It means the office, stations, etc., formed by the Director-General of AIR of Union Ministry of Information and Broadcasting.

Section 2(c)-"Broadcasting"

It means transmission of any signals, writings, pictures, images and sounds by electro magnetic waves through space or cables which is received by general public directly or indirectly through the stations.

Section 2(h)-"Doordarshan"

It is also a Kendra or office formed by the Director-General of Union Ministry of Information and Broadcasting.

The main feature of Broadcasting is that it merges Radio and Television together.

Section 3-The Prasar Bharti Board

The corporation is established under the statute. It consists of a Presiding Chairman, 8 members and 6 part-time members.

Section 12-Functions and Powers of Corporation

The main functions are:

- ☞ The primary duty of corporation is to organize and conduct public service broadcasting to inform, educate and entertain the public.
- ☞ To maintain the unity and integrity of the country, and to protect the rights mentioned under the Constitution.
- ☞ To safeguard the rights of citizen and to inform the general public all matters of national, international and political interest.
- ☞ Paying special attention in field of education, health, agriculture, family welfare, science and technology so that general public should get all latest information.
- ☞ Providing special knowledge and view of the diverse cultures and languages of various regions of country.
- ☞ Also providing special knowledge of sports and games.
- ☞ Informing and stimulating the national consciousness in regard to the status and position of women and giving overview of their problems.
- ☞ To safeguard the rights of the working class people and to work for their welfare.
- ☞ To serve the rural and weaker sections of society.
- ☞ To provide special programmes and special offers for minors and tribal section of society.
- ☞ To take special interest for welfare of children and their interests.
- ☞ Providing broadcasting coverage through the choice of appropriate technology and the best use of broadcast frequencies available.
- ☞ The corporation is taking steps for establishing libraries of radio and television.

☞ They are also ensuring that broadcasting is conducted as a public service to provide and produce programmes.

☞ The corporation is also taking steps for gathering news for radio and television.

Section 13-Parliamentary Committee

The Committee is set up to oversee that the corporation is discharging its function or not. It consists of 22 members, 15 from Lok Sabha and 7 from Rajya Sabha.

Section 14-Establishment of Broadcasting Council

The Broadcasting Council is established to receive and consider complaints from any person and for the purpose of redressal. The complaints are dealt fairly and in accordance of law.

The Broadcasting Council consist of a President and 10 other members and 4 members of Parliament.

The persons alleging that functioning of the corporation is not in accordance of law and objectives may come to Broadcasting Council.

Section 23-Powers of Central Government

The Central Government has a power to give directions to the corporation in the interest of sovereignty, integrity and unity of the country and for the interest of general public. The Central Government may give directions at any time and at any issue.

Sections 32 and 33 Talks About the Rules and Regulations of Corporation

The rules of corporation are made by the Central Government according to the needs of society but the corporation may by notification, make regulations not in consistant with this Act and the rules made thereunder to perform its functions under the Act. Regulations by the corporation shall be made only with prior approval of the Central Government.

THE CABLE TELEVISION NETWORKS (REGULATION) ACT, 1995

Cable television is the media of today. The far reaching places are also connected to the cable television programming. This technology has emerged in the past 10-15 years. This Act came into force because earlier cable TV operators and subscribers were not aware of their rights and another main reason was to limit the contents so that anything shown on TV should be according to the interest of people and their rights should not be violated. Due to the enactment of this Act, there is uniformity in media.

The main definitions under the Act are:

Section 2(aa)-"Cable Operator"

It means any person who provides cable service through cable network and is responsible for the management and operation of cable television network.

Section 2(b)-"Cable Service"

It is the transmission by cables of programmes including re-transmission by cables of any broadcast television signals.

Section 2(c)-"Cable Television Network"

It is a system which consists of a set of closed transmission paths and associated signal generation, control and distribution equipment, designed to provide cable service for reception by multiple subscribers.

Section 3-It states that a person can operate a cable television network only when he is registered as a cable operator under the Act.

Section 4-Registration as a Cable Operator

By the amendment in the year 2002, Central Government makes it obligatory for every cable operator to transmit or re-transmit programmes of any pay channel through an addressable system. One or more free to air channels should also be provided by a cable operator, for a single price to the subscribers, should be included in the package. DD news, DD national channels should be shown by every cable operator. It is mandatory for every cable operator. Multiple Satellite Operators are the big cable networks.

Government is trying to progress the Cable Television Business. For this, it is necessary to check the procedure of acquiring registration and government should also set the standards to maintain the uniformity all over the country. The main interest of cable operators should not only to make profit margins, but to ensure that competitiveness does not exceed reasonable limits.

AN OVERVIEW OF THE TELECOM REGULATORY AUTHORITY OF INDIA (AMENDMENT) ACT, 2000

This Act was earlier passed in the year 1997 to overcome the problems of telecommunications. In 1990, a new phase of telecommunication was started. P.V. Narsimha Rao started the liberalization to trade barriers. National Telecom Policy was started in 1994. Later, it was further developed in 1999. Mobile phones were first introduced in 1994. Within 2 years, cell phones became a rage. Basic telephony means landlines were open to private and foreign direct investment, 24% which was increased to 49% and now it is 74%. Nokia is a part of foreign direct investment. There was no clear picture that who will decide the tariff. Now it is decided by Telecommunication Regulatory Authority of India.

Section 14-Establishment of an Appellate Tribunal

Any dispute arising will be decided by Telecom Disputes Settlement Appellate Tribunal. The seating of the tribunal is at Hotel Samrat. Its main function is to adjudicate any dispute arising:

- ↪ Between a licensor and a licensee.
- ↪ Between two or more service providers.
- ↪ Between a service provider and a group of consumers.

If any person is dissatisfied from the order of tribunal, then he has to go for an appeal to Supreme Court.

Section 14b-the Appellate Tribunal consists of a Chairperson and not more than two members to be appointed by notification by the Central Government.

Section 14c-the Chairperson is a Judge of Supreme Court or Chief Justice of a High Court. In case of the member, he must hold the position of Secretary to the Government of India.

Section 14N-Transfer of Appeals

All appeals pending before the High Court immediately before the commencement of this Amendment Act are transferred to the Appellate Tribunal.

Section 15-Civil Court does not have jurisdiction to interfere in the matters of Telecom Disputes.

Section 18-Any person aggrieved from the orders of High Court or the tribunal shall go to the Supreme Court.

© Universal law Publishing Co.

CHAPTER X

Domain Names and Domain Names Dispute Resolution

Synopsis

Trademark

Trademark Infringement

Passing Off Action

Domain Names

Domain Name Consist of Different Parts

Domain Name Distribution

Domain Name Infringements

Resolving Domain Name Disputes

Bad Faith Registration

Relevant Cases Related to Bad Faith Registration

Copyright and WIPO Treaties

Trademark

What are the rights of trademark owner?

A trademark means a mark capable of being represented graphically and may include a word, name, symbol, device, numeral, letters, pictures, signature, label, slogans, logo, shape, graphic, designs, three dimensional forms, moving image, product or packaging features, etc.

Trademark is distinctive in nature. It is distinctive of a person's goods or services and it is useful to identify the goods or services and distinguishes the goods or services of others. If two goods are same in quantity and quality, then it is the trademark which distinguishes the goods and helps the buyer to identify the goods.

In digital medium, the owner of trademark has various rights:-

- Right of goodwill or assign its goodwill value.
- Right to trade - Right to exhibit, market or promote the goods in an exclusive manner.
- Right of sole proprietorship - The owner of trademark has the right to use it in any manner; he can stop others from using the said mark or similar mark.
- Right to become a licensor - The owner of mark can issue license for a fee.
- Right to sue - The owner of mark can also initiate legal action against the infringer. He can also institute legal proceedings in both Civil and Criminal Courts.

The trademark is not a legal person. It is the owner of the trademark who is a legal person.

Trademark Infringement

When it can be said that the owner of trademark is infringed?

A trademark infringement is a violation of the trademark owner's right. An infringement occurs only when the trademark cause deception or confusion or mistake in the minds of persons who are using the goods or services of similar

trademark.

Sellers of goods make a trademark which is similar to the trademark of branded goods or services.

Passing Off Action

What do you mean by passing off action? Explain its two broad categories?

It comes under common law. It totally depends on the principle that no one has any right to represent his goods, as similar to other person's goods. Trader of goods misrepresented his goods to the customers so that customer can purchase those goods which are similar to those branded goods and trademark is also similar to those goods so that it can cause confusion in mind of customers. It is treated as a form of unfair competition. It can also be said that customers wrongfully identify the goods.

TWO BROAD CATEGORIES OF PASSING OFF ARE:-

1. In the first category, it is alleged that the defendant (trader) has promoted his business or goods in such a manner which creates false impression, mistake, confusion in the minds of customers and has proved that his business is authorized or approved by plaintiff (whose trademark is infringed) and that there is some business connection between them. The defendant has created the false impression in order to earn more money and to gain goodwill of another.

2. In second category, the competitors are engaged in same business and plaintiff complains that defendants (competitors) have named, packaged or described his product in same manner so that it creates the confusion in mind of customers that defendant product or business is same to that of plaintiff.

The right of trademark owners to own, license, sell, exhibit, promote are threatened/misused by web based technology tools like search engines, meta tags and hyper links.

Domain Names

Domain names are alpha numeric designation which is registered or authorized by the Registrar of Domain Names, Domain Name Registry or other Domain Name Registration Authority as part of an electronic address on internet.

Domain names provide a system of internet address which can be translated by the Domain Name System (DNS) into numeric address Internet Protocol (IP) used by network.

For example: When we press Enter, a number comes i.e., 202.12.45.65 in an alpha numeric form of www.specimen.com known as Domain Name System.

Domain Name is a kind of a web address of a website.

Domain Name Consist of Different Parts

1. Secondary Level Domain names (SLD) - It can be chosen by the person registering the name. It is also called as middle name, i.e., specimen.

• .com is a suffix which is assigned at the end of the websites.

2. The other part which is used throughout the world are "Top Level Domain". These are known as g TLDs i.e., "generic" Top Level Domains.

Earlier there were seven g TLDs (.com, .edu, .gov, .int, .mil, .net or e.org). Seven more g TLDs are .aero, .biz, .coop, .info, .museum, .name, .pro

By 80s or 90s we only had .com, but by early 1990s other Top Level Domains were also introduced. Names have been assigned to the country of origin. For example, in for India, .us for United States, .ca for Canada, .jp for Japan, .de for Germany, .uk for United Kingdom, .sg for Singapore, etc. They are known as cc TLDs i.e., country code Top Level Domains.

The National Internet Exchange of India (NIXI) has been set up to facilitate the exchange of internet within the country. It has also set up the country code Top Level Domain i.e., in registry by the Government of India.

Domain Name Distribution

The registration of Domain Name has been done by Network Solutions Inc. (NSI) since 1992 under an agreement with National Science Foundation and the U.S. Department of Commerce. In 1999, the Internet Corporation for Assigned Names and Numbers (ICANN), a private sector corporation based in Marina Del Rey, California, USA, took over the management of Domain Name System from NSI.

ICANN performed many functions. The main functions are:-

1. Setting up of rules for giving the numbered IP address/Protocol Parameters. Numbered addresses are given to the registries by ICANN. There are three registries in the world.

- American Registry for Internet Numbers (ARIN).
- Reseaux IP Europeens (RIPE).
- Asia Pacific Network Information Center (APNIC).

2. Adding new suffixes to the directory.

3. Setting up of rules for arbitrating disputes over Domain ownership. ICANN has adopted WIPO report for trademark related Domain Name Disputes and has framed Uniform Domain Name Dispute Resolution Policy.

Domain Names are allotted by the Registrar of Domain Name Registry (DNR) on first come first served basis. Domain Name can be registered in an on-line medium as well. For example www.networksolutions.com, www.net4india.com.

Domain Names can be registered for one year, two years and upto 10 years maximum. There is no limitation as for the length of alphabets or words in the secondary level domain. Secondary level domain can be alpha numeric name as well. E.g., 123india.com, www.net4india.com.

While going for a registration, a person who is registering a domain name is known as registrant and he is obtaining a domain name from the domain name registrar. That means there exist a contract between a Registrant and a Registrar. Since Domain Names are given or distributed on first come first served basis, it has resulted in domain name cyber squatting by certain individuals.

Domain Name Infringements

What are the domain name infringements?

1. Cyber Squatting.
2. Typo Squatting.
3. Cyber Smearing.

The Domain Names which are given or distributed on first come first served basis, has resulted in Cyber Squatting by certain individuals. The Cyber Squatters book the Domain Names of well known companies, famous trademarks including celebrities name and then ask for fabulous amount to vacate such domain names.

Cyber squatters can also indulge in other activities like Typo Squatting and Cyber Smearing.

Cyber Squatting	Typo Squatting	Cyber Smearing
Tata sons, A person who is not a team owner of	www.disney.com . A typo squatter may take a site by	Certain sites which may be called as hate sites or smear sites of well-known

Tata sons may take a domain name as www.tatasons.com. By having this domain name, this person would be impersonating Tata sons and their goodwill in the cyber space which could be detrimental to the Tata sons and its various affiliates/companies.	the name www.disney.com. That means a typo squatter is assuming that a user of net while typing www.disney.com may type or may misspell Disney as disney which means a typo squatter would be diverting a traffic of user who are interested in visiting disney.com may find themselves at disney.com.	companies. For example: Kentukey fried chicken has a smear site by the name of kentucky fried chicken sux.com runs a smear campaign against kentucky fried chicken and its commercial practices. For example: This hate site tells how kentucky fried chicken ill-treats their chicken. Kentukey fried chicken sux.com is an initiative of a society which is working towards stopping cruelty towards birds and chickens.
---	---	---

Resolving Domain Name Disputes

Domain Name Disputes are resolved under a policy referred as UDRP (Uniform Domain Name Dispute Resolution Policy) is created by ICANN (Internet Corporation of Assigned Names and Numbers), in association with WIPO (World Intellectual Property Organization).

Under UDRP, a domain name registered by a registrant can be cancelled or suspended if it is proved that the registrant has obtained the domain name in bad faith as defined under UDRP.

There are four Domain Name Dispute Resolution Service providers:-

1. WIPO (World Intellectual Property Organization)-It is effective from 1st December, 1999.
2. CPR (Institute for Dispute Resolution)-It is effective from 22nd May, 2000.
3. NAF (National Arbitration Forum)- It is effective from 23rd December, 1999.
4. ADNDRC (Asian Domain Name Dispute Resolution Centre)-It is effective from 28th February, 2002.

There was another Domain Name service provider by the name of e-Resolutions and they had to close their operations. The Domain Name Dispute Resolution Service Providers provide Dispute Resolution services in an on-line medium and maintain harmony and friendly relations.

Complainant has an option to approach any one of the forums and file a complaint. On receiving the complaint, such dispute resolution service providers will appoint an arbitrator or panel of arbitrators to look into the complaint. A copy of complaint is sent to the offender for his response. On receipt of the response, the arbitrators will decide whether the complaint has a merit or not and decide accordingly. The entire process of an on-line arbitration which may also be called as on-line dispute resolution may take 6-9 months to complete and may cost upto US dollar 500. If the arbitrators feel that the case relates to bad faith registration then they may order transfer of that disputed domain name from respondent to the complainant. The difference of UDRP with the trademark legislation is in the sense that under UDRP, there are no civil damages or compensation given to the complainant if it is proved that it was a bad faith registration on the part of the respondent. Trademark legislation talks about both civil and criminal liabilities against infringer. UDRP does not mention any criminal prosecution of the offender or infringer.

The domain name registrant has to submit a mandatory administrative proceeding in the event that the third party (a complainant) asserts to the applicable provider that:-

1. The registrant domain name is similar to a trademark in which the complainant has rights.
2. The registrant has no rights or interest in domain name.
3. The registrant domain name is registered and used in bad faith and obtained with fraud.

In the administrative proceeding, the above mentioned elements must be proved.

Bad Faith Registration

What is bad faith registration?

1. The registrant has registered the domain name for the purpose of selling, renting or transferring the domain name registration to the complainant who is the owner of the trademark or competitor of the complainant for valuable consideration.
2. The registrant has registered the domain name to prevent the owner of trademark from reflecting the mark in corresponding domain name and the registrant must be engaged in same business.
3. The registrant has registered the domain name in order to disrupt the business of a competitor. It was the principle laid down in *www.rediff.com* case. This case was decided in Bombay High Court. This is the first example of Typo Squatting.
4. The registrant has used the domain name in order to attract, for commercial gain and to create confusion with the complainant's mark as to the source, sponsorship, endorsement of its registrant website or of a product or service on the registrant's website or location.

Many rules have been set up by nations based on UDRP to resolve the country specific domain name disputes. The rules of UDRP have been accepted and the global expansion of rules of UDRP is because of its simplified procedure and it is easy accessible. This is on-line dispute mechanism and it is also good revenue model for the dispute resolution service providers.

No domain names are for life. One has to register the domain name again after the period ends and renew it again. Once it is not renewed it is open to every person.

There is no such bar of getting the domain name registered as domain name in the digital medium. There can be many mode of communication available to a person to have a desirable domain name. For example: if ICICI Bank owns a domain name like *www.icicibank.com* then any person may have a registration that may include ICICI bank as a secondary level domain in any manner whatsoever.

Other case on respect of bad faith registration is *www.sify.com* case. Person used domain name in name of *www.sify.com*. Supreme Court ruled that by giving *sifynet.com*, the respondent or accused in this case is trying to create confusion in mind of user. Phonetic similarity is there. This case was decided in the year 2004.

Mutual funds case is also another example of Typo Squatting. A person was using *www.mutualfundofindia.com* a registered site by proprietor. In order to create confusion in mind of other consumers, accused made a site *www.mutualfundsofindia.com*.

Relevant Cases Related to Bad Faith Registration

Bennett Coleman and Co. Ltd. v. Steven S. Lalwani, Case No. D 2000-0014.

It was contended by the complainant that the respondent registered the domain names "*theeconomicstimes.com*" and "*thetimesofindia.com*" which was same to the plaintiff's domain name i.e., "*economicstimes.com*" and "*timeofindia.com*" and represented its electronic publications of its leading print newspapers. It was also contended that the domain names of the defendants again directed the internet users to the respondent website "*indiaheadlines.com*" which provides news related to India. It was also held that the WIPO panel confirmed the presence of three elements as stated in UDRP and ordered the respondent to transfer the domain name to the plaintiff.

Similarly, in *Tata Sons Ltd. v. The Advance Information Technology Association*, Case No. D 2000-0049 the WIPO panel found the presence of all three elements as stated in UDRP. Therefore, it was stated that the respondent registrant of "*tata.org*" has no right or interest in the said domain name and the domain name should be transferred to the plaintiff.

Other cases related to bad faith registration in which the domain name was similar to the plaintiff's domain name and court ordered to transfer the domain name to plaintiff are:

In Mahindra Corporation v. Amit Mehrotra, the domain name involved was "Microsoft.org".

In Mahindra and Mahindra Ltd. v. Neoplanet Solutions, Case No. D 2000-0248 the domain name involved was "mahindra.com".

In Castrol Ltd. v. Shrinivas Ganediwal, in this case, the domain name involved was "castrolindia.com" and all three elements of UDRP were found in this case also. Therefore, court ordered to transfer the domain name to plaintiff.

In Asian paints (India) Ltd. v. Domain Administration, Case No. D 2002-0649 it was held in this case that the registration of domain name "asianpaints.com" is similar to the complainant domain name and due to this similarity, the domain name of respondent is creating confusion in mind of people. It was also observed that the respondent have no explanation or reason for registering the similar domain name to that of plaintiff and have no interest or right in it. The website of complainant is www.asianpaints.com and respondent has omitted the letter "S" in order to create confusion and exploit users.

In Yahoo Inc. v. Akash Arora, 1999 ALR 620 the defendant was using the domain name "yahooindia.com" in which the content and colour scheme was similar to the plaintiff's "yahoo.com". It was observed by Dr. M.K Sharma, J., High Court that "if an individual is a sophisticated user of the internet, he may be an unsophisticated consumer of information and such a person may find his/her way to the different internet site which provides almost similar type of information to that of plaintiff and creates confusion in mind of person who intends to visit the internet site of the plaintiff but due to confusion, he reaches to site of defendant".

How the distinctiveness is acquired? Explain with case laws?

For the registration of domain name or trademark, distinctiveness is required. Distinctiveness may be either inherently distinctive or may acquire distinctiveness through secondary meaning (in market place).

In Dr. Reddy's Laboratories Ltd. v. Manu Kosuri, 2001 (3) Raj 122 it was observed by Delhi High Court that the plaintiff holds the trademark in name of DR. REDDYS and it has acquired distinctiveness through a secondary meaning. Defendant registered the mark as "drreddyslab.com" which is identical to the mark of plaintiff and it creates confusion in mind of internet users.

In Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd., MANU/SC/0462/2004 : AIR 2004 SC 3540: (2004) 6 SCC 145, it was held before the Court that the same domain name causes confusion in mind of internet users and which results in accessing one domain name instead of another by users.

The facts of the case are the appellant was incorporated in the year 1995 and registered the domain name like www.sify.net, www.sifymall.com, www.sifyrealestate.com in June, 1999. The appellant contended that the word "sify" is invented by using the same elements of its corporate name, Satyam Infoway. The appellant also stated that its name and goodwill exist in the name "sify" only.

The respondent was carrying his business in name www.siffynet.com and www.siffynet from May, 2001.

It was opined by Ruma Pal, J., that there is a similarity between two words "sify" and "siffy" which creates confusion in mind of internet users. The similarity in the name may lead the user to think that there is a business connection between the two. Therefore, only by using the letter "F" may create confusion in mind of internet users and user will get the services of respondent of which he may be disappointed with the result. Similar domain name also lead user to receipt of unsought for services and he may not be satisfied from services.

Supreme Court also concluded that the respondent is using similar domain name as of appellant and is using appellant reputation. The investments made by appellant in his trade name is being used by respondent, therefore, appellant is entitled to get claim.

Write a note on WIPO?

WIPO copyright treaty came into existence on 20th December, 1996. Another treaties are WCT i.e., WIPO Copyright Treaty, 1996 and WIPO Performers and Phonogram Producers Treaty. By virtue of these treaties, the copyright regime has also been extended to cover the digital medium as well.

The WCT protects literary and artistic works such as books, computer programs, music, photography, paintings, sculpture and films.

The WPPT protects the rights of producers of phonograms or sound recordings. E.g., CDs, Cassettes, as well as the right of performs in which performance of performers are there in sound recordings.

Both treaties provide the right which allows the creators to control or be compensated for the ways in which their creations are misused or enjoyed by others. These treaties have provided not only the copyright protection to the performers and phonogram producers but also to the broadcasting organizations. These treaties have also introduced a term called Digital Rights Management (DRM) which means a copyright holder has a right to protect and manage his creations by using technological tools to encrypt the data or content from being infringed. One cannot decode the encrypted material.

WCT or WPPT are applicable with all digital technologies and media. The result of these WIPO initiatives (i.e., WCT and WPPT) is that there is now legal clarity regarding the rights granted to the authors, performers and producers in digital medium. These treaties also provide legal protection and remedies against technological measures that are used by authors, publishers and other rights owners to protect their intellectual property.

Copyright and WIPO Treaties

India became party to the Berne Convention for the protection of literary and artistic works on April 1, 1928, also to the Paris Act (of July 24, 1971, as amended on September 28, 1979) on May 6, 1984, articles 1 to 21 of the treaty. India is also Party to the Universal Copyright Convention, 1952. Though India is not still party to either WCT or WPPT but it extends the reproduction rights to digital environment by virtue of article 9 of The Berne Convention. Authors of literary and artistic works are protected by this convention. Article 9 of the Berne Convention also become part of the Copyright Act in 1994 as section 14(a)(i) which explains the meaning of copyright. "Copyright" means the exclusive right subjected to the provisions of this Act, to do or authorise the doing of any of the following acts in respect of a work or any substantial part of it.

In case of literary, artistic or dramatic works:

- 1.To reproduce the work in any form.
- 2.To issue copies of work in any form.
- 3.To perform work in public and communicate to public.
- 4.To translate or adapt the work.
- 5.To sell, hire, offer to sell the work.

The Copyright Act needs amendments to make it compatible with WCT and WPPT. The inadequacies must be addressed and necessary amendments should be introduced.

CHAPTER XI

ADVANCED TECHNOLOGY

SYNOPSIS

The Protection of Plant Varieties and Farmers' Rights Act, 2001

Important Definitions under the Act are as Follows

Section 2(j) Defines Extant Variety Available in India

Section 2(k) "Farmer"

Section 2(l) "Farmers' Variety"

Section 2(za) "Variety"

Section 12. Registry

Section 13. National Register of Plant Varieties

Chapter III of the Act Talks About Registration of Plant Varieties and Essentially Derived Variety

Section 14. Application for Registration

Section 15 Registrable Varieties

Section 16 Persons who may make Application

Section 18 Form of Application

Section 19 Test to be Conducted

Section 21 Advertisement of Application

Chapter IV of the Act Deals with Duration and Effect of Registration and Benefit Sharing

Section 24 Issue of Certificate of Registration

Section 26 Determination of Benefit Sharing by Authority

Section 30 Researcher's Rights

Chapter VI Talks About Farmers' Rights

Section 31 Farmers' Rights

Section 41 Rights of Communities

Gene Fund

Section 45 - Gene Fund

Chapter VII of the Act Deals with Compulsory Licence

Section 47 Power of Authority to Make Order for Compulsory License

Section 50 Duration of Compulsory License

Chapter VIII of the Act Deals with Plant Varieties Protection Appellate Tribunal

Chapter X of the Act Explains Infringement, Offences, Penalties and Procedures

Section 64 Infringement by a Person

Section 65 Suit for Infringement

Section 66 Relief in Suit for Infringement

The Biological Diversity Act, 2002

Chapter VI of the Act

Chapters VII and VIII Talks About Finance, Audits and Accounts

Chapter X section 41 of the Act Deals with Biodiversity Management Committee

Chapter XII Miscellaneous

Section 50 - Settlement of Disputes

Section 55 - Penalties for Contravening Provisions of

THE PROTECTION OF PLANT VARIETIES AND FARMERS' RIGHTS ACT, 2001

Important Definitions under the Act are as follows

Section 2(c). "Breeder" means a person or group of persons or a farmer or group of farmers or any institution which has bred, evolved or developed any variety.

Section 2(j). Defines extant variety available in India

- (i) it is notified under section 5 of the Seeds Act, 1966;
- (ii) farmers' variety;
- (iii) a variety about which there is common knowledge;
- (iv) any other variety which is in public domain.

There is no IPR about a variety which is in common knowledge and which is in public domain.

Section 2(k). "Farmer"

The category of farmer as defined under the Act is extremely wide.

Farmer means any person who:-

- (i) cultivates crops either by cultivating the land himself; or
- (ii) cultivates crops by directly supervising the cultivation of land through any other person; or
- (iii) conserves and preserves, severally or jointly, with any person any wild species or traditional varieties or adds value to such wild species or traditional varieties through selection and identification of their useful properties.

Section 2(l). "Farmers' variety"

As a breeder, if any variety is cultivated then there will be an IPR but for farmer's variety there is no IPR. The main ingredients of this section are-

1. farmer's variety means a variety which:-

- ❶ is traditionally cultivated;
- ❷ is evolved by the farmers;
- ❸ is a variety about which the farmers possess the common knowledge.

Section 2(za). "Variety"

This section is very general. This section exclude micro-organism.

Variety means a plant grouping:

- (i) It is defined by the expression of the characteristics resulting from a given genotype of that plant grouping.
- (ii) It is distinguished from any other plant grouping by expression of at least one of the said characteristics.
- (iii) It is considered as a unit with regard to its suitability for being propagated, which remains unchanged after such propagation, and includes propagating material of such variety, extant variety, transgenic variety, farmers' variety and essentially derived variety.

Section 12. Registry

This section talks about registry of plants varieties. Registry is established by Central Government. Registrar is also appointed for this purpose.

The head office of the Plant Varieties Registry shall be located in the head office of the Authority, and for the purpose of facilitating the registration of plant varieties.

Section 13. National Register of Plant Varieties

It is kept at the head office of the registry. The register shall be kept under the control and management of the Authority.

The register of plant variety contains-

- ❧ Names of all the registered plant varieties with the names.
- ❧ Names and addresses of their respective breeders.
- ❧ The right of such breeders in respect of the registered variety.
- ❧ The particulars of each registered variety.
- ❧ Its seeds or other propagating material along with salient features.

CHAPTER III OF THE ACT TALKS ABOUT REGISTRATION OF PLANT VARIETIES AND ESSENTIALLY DERIVED VARIETY

The registration of plant variety is done in order to prevent IPR of derived variety.

Section 14. Application for Registration

An application should be made to Registrar for registration of any variety. The variety to be registered is any:-

- (a) genera and species.
- (b) extant variety.
- (c) farmers variety.

Section 15. Registrable varieties

This section talks about the registrable variety, i.e., any new variety or extant variety shall be registered under the Act only if it has criteria of novelty, distinctiveness, uniformity and stability.

A new variety is novel if it has not been sold or disposed of before the date of filing of an application.

The variety should be distinct from any another variety. It should have one special characteristic feature. The variety

should be uniform in its essential characteristics.

The variety should be stable, if its essential characteristics remain unchanged after repeated propagation.

A new variety shall not be registered if it:-

- (i) is not capable of identifying such variety,
- (ii) consists solely of figures,
- (iii) is liable to mislead or to cause confusion concerning the characteristics,
- (iv) is likely to deceive the public or cause confusion in the public regarding the identity of such variety,
- (v) is likely to hurt the religious sentiments of citizens of India,
- (vi) is prohibited for use as a name or emblem for any of the purpose,
- (vii) is comprised of solely or partly of geographical name.

Section 16. Persons who may make Application

An application for registration made by-

- (a) the breeder of the variety, or
- (b) any successor of the breeder, or
- (c) the assignee of the breeder, or
- (d) any farmer or group of farmers, or
- (e) to make application on his behalf.
- (f) any university or publicly funded agricultural institution.

Section 18. Form of Application

An application should contain:-

- (a) name of variety,
- (b) the denomination assigned to such variety by the applicant,
- (c) affidavit sworn by the applicant that such variety does not contain any gene,
- (d) it should be according to regulation,
- (e) contain a complete passport data of the parental lines from which the variety has been derived along with the geographical location in India from where the genetic material has been taken and all such information relating to the contribution, if any, of any farmer, village community, institution or organization in breeding, evolution or developing the variety,
- (f) it should contain statement of its characteristics of novelty, distinctiveness, uniformity and stability as required for registration,
- (g) accompanied by such fees as may be prescribed,
- (h) contain a declaration that the genetic material or parental material acquired for the breeding, evolving or developing the variety has been lawfully acquired.

Section 19. Test to be Conducted

A particular quantity of seeds should be made available to Registrar along with application. It should be provided for conducting test to evaluate the conformity of seed standard with the parental material.

Section 21. Advertisement of Application

After accepting the application by Registrar, the Registrar should advertise an application for objection. If any person will have an objection then he has to file it within three months. A copy of notice of the opposition should be served to an applicant by Registrar within two months. After receiving notice, an applicant should send a counter-statement to the Registrar, then, Registrar should send the copy to the person giving notice of opposition. It is totally binding upon the Registrar to decide whether the registration should be permitted or not.

CHAPTER IV OF THE ACT DEALS WITH DURATION AND EFFECT OF REGISTRATION AND BENEFIT SHARING

Section 24. Issue of certificate of registration

This section states that when the variety is registered then Registrar should issue certificate of registration to the applicant.

Total validity of variety are:-

VARIETIES	TIME PERIOD
Trees And Vines	18 Years
Extant Variety	15 Years
Other Varieties	15 Years

Section 26. Determination of Benefit Sharing by Authority

✎ The Authority have to publish contents of the certificate and invite claims of benefit sharing to the variety registered.

✎ On invitation of the claims, any person or group of persons or non-governmental organization will submit its claim of benefit sharing.

✎ A copy of claim is sent to breeder of variety by the authority concern. After receiving the copy of claim, the breeder will send the opposition to such claim.

✎ The authority should mention the amount of benefit sharing while disposing claim.

✎ Two things authority has to take in consideration:

☞ The nature and extent of use of genetic material of claimant in development of variety.

☞ Market value and demand of variety.

Section 30. Researcher's Rights

1.This Act does not allow any person to use variety for conducting experiment or research.

2.This Act also does not allow any person to use variety as an initial source of variety for the purpose of creating other varieties.

Proviso of the Act states that the authorization of the breeder of a registered variety is required only when there is repeated use of such variety for commercial purpose.

CHAPTER VI TALKS ABOUT FARMERS' RIGHTS

Section 39. Farmers' Rights

Rights of farmers are:-

- (i) a farmer who has bred or developed a new variety shall be entitled for registration and other protection under this Act,
- (ii) a farmer who is engaged in the conservation of genetic resources of land races and wild relatives of economic plants is entitled for recognition and reward from the Gene Fund.
- (iii) A farmer shall be deemed to be entitled to save, use, sow, re-sow, exchange, share or sell his farm produce including seed of a variety in the same manner as he was entitled before the coming into force of this Act. Provided that the farmer shall not be entitled to sell branded seed of a variety protected under this Act.

Branded seeds are defined under the Act as any seed put in a package or any other container and labeled in a manner indicating that such seed is of a variety protected under this Act.

Where any propagating material of a variety has been sold to a farmer or a group of farmers and it is disclosed by breeder of such variety to farmer that under given conditions the propagating material fail to provide such performance then farmer may claim compensation before the authority.

Section 41. Rights of Communities

A claim can be filed by:-

- (1) Any person, group of persons,
- (2) Any governmental or non-governmental organization,
- (3) Any village or local community in India.

A claim is filed for the evolution of any variety for the purpose of staking a claim on behalf of such village or local community.

The Centre notified for this purpose to report its findings to the Authority, which in turn may issue notice to the breeder of that variety.

The Authority may grant a sum of compensation to such people and that compensation shall be deposited by breeder in the Gene Fund.

Gene Fund

Section 45. - Gene Fund

What is Gene Fund?

Gene Fund is defined under the Act.

The Central Government has constituted a Fund which called as National Gene Fund.

It consists of:-

- (a) The benefit sharing which is received from the breeder.
- (b) The annual fee payable to the Authority by way of royalty.
- (c) The compensation deposited under section 41.
- (d) The contribution from national and international organization.

Section 47. Power of Authority to make Order for Compulsory License

Authority has the power to grant license after the expiry of three years from the date of issue of a certificate of registration of a variety. A person has to make an application to the Authority alleging that the reasonable requirements of the public for seeds or other propagating material of the variety have not been satisfied, the demands of the public are not fulfilled and that demand is satisfied because of the reason of increase in price. The authority then orders such breeder to grant a license to the applicant.

Section 50. Duration of Compulsory License

What is the duration when compulsory license is obtained?

The duration of the compulsory licenses shall be determined by the authority. Such duration may vary from case to case but in any case, it should not exceed the total remaining period of the protection of that variety.

CHAPTER VIII OF THE ACT DEALS WITH PLANT VARIETIES PROTECTION APPELLATE TRIBUNAL

SECTION	HEADING	EXPLANATION
54	Tribunal	The Central Government has established a Tribunal known as the Plant Varieties Protection Appellate Tribunal.
55	Composition of Tribunal	Tribunal consist of a Chairman, JudicialMembers and Technical Members as the Central Government may deem fit to appoint.
56	Appeals to the Tribunal	From the order of decision of Authority orRegistrar, the appeals are made to tribunal within prescribed period.

CHAPTER X OF THE ACT EXPLAINS INFRINGEMENT, OFFENCES, PENALTIES AND PROCEDURES

Section 64. Infringement by a Person

Infringement to variety can be caused by any person.

- (a)The person who is not the breeder of a variety registered or a registered agent or registered licensee of that variety.
- (b)That person uses, sells, exports, imports or produces such variety without the permission of its breeder.
- (c)That person has produced, use, sell other variety similar or identical to the denomination of a variety registered.
- (d)This Act is done by the person to cause confusion in the mind of general people in identifying the variety.

Section 65. Suit for Infringement

No suit shall be filed for the infringement of a variety registered under this Act, or relating to any right in a variety registered under this Act. The suit shall be instituted in any court inferior to a District Court but within the local limit of whose jurisdiction the cause of action arises.

Section 66. Relief in Suit for Infringement

The relief which is granted by court in suit for infringement includes injunction and at option of the plaintiff, either damages or share of the profits.

Penalties under the Act are as follows:-

SECTION	HEADING	PENALTY
70	P e n a l t y for applying false denomination.	Imprisonment for a term which shall not be less than three months but which may extend to two years or with fine which shall not be less than fifty thousand rupees but which may extend to five lakh rupees or both.
72	P e n a l t y for falsely representing a variety as registered.	Imprisonment for a term, which shall not be less than six months and may extend to three years, or with fine which shall not be less than one lakh rupees but which may extend to five lakh rupees, or with both.

THE BIOLOGICAL DIVERSITY ACT, 2002

Why biological diversity is creating?

It takes 1000 years to create a new variety of plants. So, Gene Pool is diversified. Innovations are made and many varieties appear or disappear. It is necessary for a human being that we should not disturb our nature i.e., our Gene Pool. Our environment should be free from pollution and human beings should not imbalance nature by doing various harmful activities. If we interfere with our nature, it will get disturbed and our new varieties will get toxins and will disappear day-by-day.

Preamble of the Act is dietary in nature. It provides for conservation of biological diversity which is an essential part of our environment. It also provides for sustainable/efficient use of its components and fair and equitable sharing of the benefits arising out of the use of biological resources, knowledge and other matters related to biological diversity.

The knowledge of local communities, farmers, and indigeneous people on how to use the many forms and type of biological resources and also how to conserve these resources is now been recognized as critical to future development and even survival of human kind.

Therefore, for the development and survival of human beings the role and importance of traditional knowledge is extremely important. Traditional knowledge is to be maintained in social and economic context in which it develops and is applied has to be maintained. The rights of local communities to their resources and knowledge have to be recognized and respected. Their views should be taken to utilize the resources. Misappropriation of these rights can erode the paces of traditional knowledge and thus adversely affect the prospects of sustainable development.

Explain the concept of bio piracy?

Bio Piracy means misappropriation of traditional biodiversity knowledge by multinationals, research institutes and breeders. In concept of bio piracy, countries, mainly the developed countries, are giving patents to genetically modified organisms. In many cases, patents on living organisms is also being given. It is important to note that companies are being given patents on genes extracted from a plant variety. That means by indulging in Bio piracy companies are decoding and identifying the best plant genes, and thereby creating monopoly rights over such genome. The development of many varieties of world staple foods like wheat, rice, maize, oats, etc., have been carried out by the farmers in developing countries over the generations through cross breeding. The multinational companies are using the traditional knowledge of communities and extracting genes and patenting such genome maps for their own benefits.

Note on bacillus thuringiensis

Bacillus thuringiensis is a naturally occurring soil bacterium which produces a protein fatal to many insects that consumes it. It has been used as a biological pesticide by farmers since 1940's. Companies have now genetically engineered the bacillus thuringiensis gene in crops including maize, soyabean, cotton, potato, rice

so that the plants produce their own insecticides. By granting patent to bacillus thuringiensis gene, a bio piracy element is introduced in patents. Moreover, these types of crops are environmentally harmful. In studies at Cornell University USA it was shown that pollen from bacillus thuringiensis maize killed Monarch Butterfly Larvae that ingested in laboratory conditions.

Overview of Act

Section 2 of the Biological Diversity Act, 2000 is about various definitions.

Section 2(b) - "Biological Diversity" means the variability among living organisms from all sources and the ecological complexes of which they are part and includes diversity within species or between species and of eco-system.

Section 2(a) - Defines "Benefit Claimers". All tradition knowledge holders communities come under benefit claimers category.

Section 2(c) - "Biological Resources" means plants, animals and micro organisms, their genetic material and by products. E.g., Cheese, curd etc., with actual or potential use or value, but does not include human genetic material.

Section 2(o) - "Sustainable Use" means the use of components of biological diversity in such manner that does not lead to long-term decline of the biological diversity and maintaining its potential to meet the needs and aspirations of future generations.

Section 2(p) - Defines "value added products" which means those products which contain extracts of plants and animals in unrecognizable and irreparable form. E.g. Jelly, silk, mushroom, etc.

Who has to seek permission from the national biodiversity authority?

Section 3 - "Regulation of Biodiversity Authority"- Without the approval of National Biodiversity Authority, persons cannot undertake Biodiversity related activities. They have to seek permission from the National Biodiversity Authority.

- A person who is not a citizen of India.

- A citizen of India who is non-resident.

- A body Corporate, association or organization which is not incorporated in India or is incorporated in India which has any non- Indian participation in its share capital or management.

Section 6 - Application for Intellectual Property Rights not to be made without approval of NBA.

It is mandatory to get approval from NBA for any Intellectual Property Right for any research or information on biological resource.

NBA also grants royalty, fee or share in profit arising from commercial utilization of rights.

Section 7 - Intimation to State Biodiversity Board for obtaining Biological Resource for commercial or any utilization, it is also necessary to give prior intimation to State Biodiversity Board. The provision of this section does not apply to local people and communities of area, cultivators, vaid, hakims, who have been practicing indigenous medicine.

Section 8 - The head office of National Biodiversity Authority is at Chennai and it consist of Chairperson and 15 other members.

Section 13 - Committee of NBA deals with Agro- Biodiversity which means biological diversity of agriculture related spices and their wild relatives.

Section 18 - Of the Act talks about functions and powers of NBA i.e., to issue guidelines for access to

biological resources and for fair and equitable benefit sharing. NBA also advise the Central Government on conservation of biodiversity, sustainable use of its components and equitable sharing of benefits, etc.

NBA on behalf of Central Government also take measures to oppose the grant of intellectual property rights outside India on biological resource which is obtained from India or derived from India.

Section 19 - To obtain any biological resource or a patent or any other form of intellectual protection, any person should make an application to NBA and should get its approval.

Section 20 - Once the biological resource or knowledge is obtained with approval of NBA then no person can transfer it to any other person except with the permission of the NBA.

Explain determination of equitable benefit sharing by NBA? In what manner it can be given effect?

Section 21 - Determination of equitable benefit sharing by NBA- It ensures that the terms and conditions on which approval is granted secures equitable sharing of benefits arising out of the use of biological resources, products between benefit claimers, persons who apply for approval, etc.

Manner in which it gives effect are:

- ☞ Grant of joint ownership of Intellectual Property Rights to NBA or where benefit claimers are identified to such benefit claimers.
- ☞ Transfer of technology.
- ☞ Location of production, research and development units in areas which facilitate better living standard to benefit claimers.
- ☞ Association and unity among benefit claimers, Indian Scientists and the local people. Their views should be taken in production.
- ☞ Funds are collected for aiding benefit claimers.
- ☞ Payment of monetary compensation and non-monetary benefits to benefit claimers as NBA may deem fit. Compensation is paid to benefit claimers if any wrong is done to them.

CHAPTER VI OF THE ACT

This chapter talks about State Biodiversity Board. It is established under section 22 of the Act. The main aim of State Biodiversity Board is to assist National Biodiversity Board in granting intellectual property rights and benefit sharing of benefits arising out of use of biological resources, their products, etc.

Section 23 talks about functions of State Biodiversity Board which is almost similar to National Biodiversity Board.

CHAPTERS VII AND VIII TALKS ABOUT FINANCE, AUDITS AND ACCOUNTS

This chapter talks about Finance, Audits and Accounts of NBA and State Biodiversity Board respectively, for which an accountant is hired who maintains register of all biological resources which are sold and purchased and calculated the profits for NBA and State Biodiversity Board. Accountant also has to maintain account books/registers and should give details to NBA and State Biodiversity Board time to time.

What are the duties of Central and State Governments mentioned under Chapter IX of the Act?

Write a note on biodiversity Management Committees?

Section 36 - Central Government should develop National Strategies, plans, etc., with the consultation of benefit claimers, local people and Indian scientists for conservation of biological diversity and sustainable use of biological resources.

Section 37 - Central Government and State Government should establish biodiversity heritage sites for local people,

benefit claimers, etc.

Section 38 - Central Government has power to notify the threatened species which are part of biological resources and they should be notified under the Act.

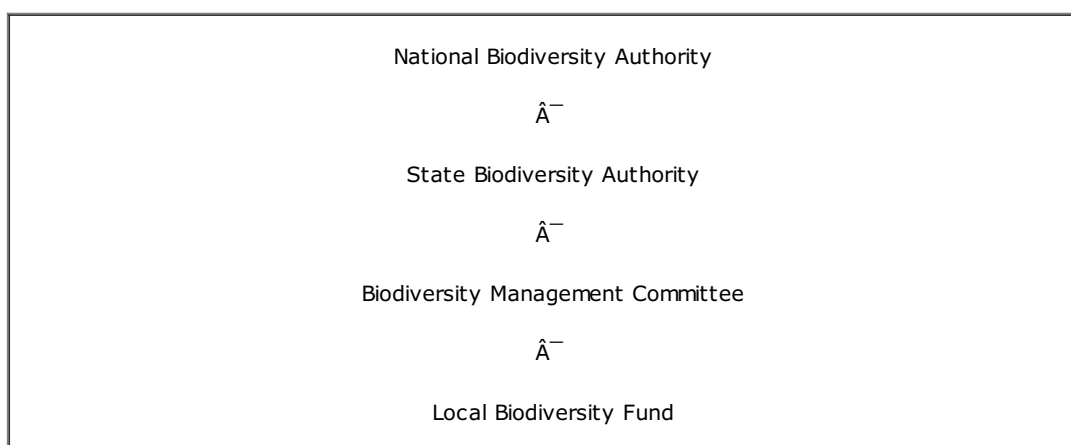
Section 39 - Central Government also has power to designate repositories.

Chapter X Section 41 of the Act deals with biodiversity management committee

Local body constitutes a Biodiversity Management Committee within its area for various purposes.

1. For promoting conservation.
2. Sustainable use of biological resources.
3. Documentation of biological diversity including preservation of habitats.
4. Conservation of landrace.
5. Conservation of folk varieties and cultivators.
6. Conservation of domesticated stocks.
7. Conservation of breeds of animals.
8. Conservation of micro-organisms.
9. Chronicling of knowledge relating to biological diversity.

Chapter XI of the Act deals with Local Biodiversity Fund. Sections 42 and 43 of the Act deals with grants to local biodiversity fund and constitution of local biodiversity fund. The main purpose of local biodiversity fund is to follow rules and regulations framed by State biodiversity fund and Biodiversity Management Committee. Local biodiversity fund is bound by these Committees and should assist them in any manner. The main motive of local biodiversity fund is to collect funds for local people for preservation of biological resources and sustainable use of biological resources.



Chapter XII MISCELLANEOUS

Section 50 - Settlement of Disputes

If a dispute arises between the National Biodiversity Authority and a State Biodiversity Board then the appeal relating to said dispute will be taken to the Central Government. The dispute can be related to any matter. If a dispute arises between State Biodiversity Board and Biodiversity Management Committee or Local Biodiversity Fund, then the dispute shall be referred by Central Government to National Biodiversity Authority.

Section 52 - Appeal -

Any person who is aggrieved by any determination of benefit sharing or order of National Biodiversity Authority or a State Biodiversity Board may file an appeal to the High Court.

Section 55 - Penalties for Contravening Provisions of

Section	Imprisonment	Fine
Section 3	Imprisonment which may extend to 5 years or	With fine of Rs. 10 lakh or both.
Section 4	Imprisonment which may extend to 5 years or	With fine of Rs. 10 lakh or extend to 5 years or both
Section 6	Imprisonment which may extend to 5 years or	With fine of Rs. 10 lakh or extend to 5 years or both
Section 7	Imprisonment which may extend to 5 years or	With fine of Rs. 3 lakh or both extend to 3 years or

Section 61 -

Cognizance of offences - No court shall take cognizance of any offence under the Act except on complaint made by,-

1. Central Government.

2. Any benefit claimer who has given notice for not less than 30 days of such offence and he has an intention to make complaint to Central Government and take the matter to Central Government or the authority or officer authorized on behalf of Central Government.

Chapter 12

Data Security And Data Protection

International Laws and Standards

International Laws

In the UK, the Data Protection Act is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. This is particularly important to ensure individuals are treated fairly, for example for credit checking purposes. The Data Protection Act states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared.

International Standards

The International Standard ISO/IEC 17799 covers data security under the topic of information security, and one of its cardinal principles is that all stored information, i.e., data, should be owned so that it is clear whose responsibility it is to protect and control access to that data.

The Trusted Computing Group is an organization that helps standardize computing security technologies.

Data Privacy and Security Concerns in Outsourcing

Indian companies are establishing India's reputation as a trustworthy outsourcing destination by proactively addressing data privacy and security concerns.

Why is data privacy and security one of the foremost concerns in outsourcing to India?

Data privacy and security are not new concepts in outsourcing. When there is transfer of sensitive and confidential information, security concerns about data leakage or misuse do arise. For anti-outsourcing lobbies, data privacy and security concerns are cited as one of the main reasons to curb outsourcing. Some consider the security risks to be the same if the data were handled offshore or onshore, while others are unsure about the data privacy and security laws in countries like India and view it as a serious deterrent to their decision to outsource.

Whether or not the security concerns are baseless, companies in the US and UK are under increasing pressure with legislations that mandate the privacy of customers' financial and medical data. Indian companies realize that they need to scale up their data privacy in order to address these security concerns before there actually turns out to be a problem. From individual companies to associations like NASSCOM, proactive measures are being taken to ensure that India's unique value proposition is "trustworthy outsourcing".

How is India dealing with data privacy and security concerns?

Most data privacy and security concerns of companies outsourcing to India are unfounded. But the Indian Government and Associations such as NASSCOM are working towards ensuring that data privacy laws in India are at par with international legislation.

NASSCOM: The National Association of Software Services Companies or NASSCOM is working with the government to address security concerns in outsourcing to India and to ensure that India's data privacy legislation is more in line with the U.S. It also intends to have the security practices of all its 860 members audited by international accounting firms. A cyber crime unit, which NASSCOM initiated in Bombay's police department where officers were trained to investigate data theft, is planned in nine other cities.

NASSCOM also encourages Indian companies to share information on back office workers, create a Certification Authority for safety and plug gaps in Indian laws by familiarizing themselves with international laws.

Proactive Data Privacy Measures in Indian Companies

Indian companies have already put in place or are currently honing their data privacy and security measures even

before the Government finishes with the legislation. Employees access their workplace with the use of swipe cards, conform to prescribed modes of data transfer and shred notes of client conversations after the shift ends. Visitors are not allowed into the working area of a BPO company. Third party call centre operations in India and back-office subsidiaries of global companies such as General Electric, are adding state-of-the-art systems to monitor phone conversations, prevent data misuse, and to ensure total compliance to data privacy and IT security measures.

A recent incident of data misuse by an employee of a well-known BPO in India has resulted in rising security concerns about outsourcing. Whether global clients dismiss it as a one-off case or the episode unleashes a fresh round of BPO backlash, it is clear that vendor companies in India are focusing not only on network safety features but also on the quality of employees that they hire. There has been an increased focus on:

Data privacy legislation: Regulatory bodies and companies are pushing for comprehensive data protection, security and privacy legislation in India along the lines of Europe, U.S. and UK to address security concerns of customers.

Technology: Companies in U.S. may want to see more investments in new technologies such as keypad authentication of PIN numbers for credit card processing, etc.

Legal enforceability of SLAs: The US and European customers will have greater confidence in Indian vendors if their contracts are made legally enforceable, both in their home country and in India.

Background checks of candidates: HR will have to adopt best practices for comprehensive screening and background checking of all new hires, as is done in countries like the U.S. and UK.

Data Privacy and Security Measures at Outsource2India

Outsource2India has made substantial budget outlays for data privacy and security. Our core team of data privacy and IT security experts has ensured that proactive processes are in place to prevent security breaches and data misuse, rather than having to address such mishaps after they arise.

O2I's well-defined data privacy and security measures are built into our processes as well as our IT infrastructure and network.

Data Security at O2I: Process

Non-disclosure/confidentiality agreements.

Audit trials for all system activities.

Access to registered and authorized users only.

Scanning of servers for penetration testing.

Data Security at O2I: Network.

Total secured CISCO VPN Tunnel to client.

Secured Cisco(r) Intelligent switches and Cisco(r) Network Assistant optimized for LAN.

Cisco(r) PIX(r) Firewall to block all ports for HTTP, FTP, TCP/IP, UDP and even ICMP.

Virtual Private Network (VPN) protection and Secure Network.

Secure network firewalls.

Secure Encrypted Web Servers and laptops.

Biometric Access.

Data Security and Privacy measures for O2I employees.

Secure Smart Card and Secure Premises Login.

Secure Remote Access (VPN).

Single sign-on to enterprise and desktop applications.

Despite technology-driven protection devices and timely detections mechanisms, we recognize that our employees' attitudes towards data privacy are key to addressing security concerns of our clients. We conduct detailed background checks on candidates before they are hired. All our employees are bound by confidentiality agreements and are adequately trained in data security processes.

Data Privacy and Security: India Initiatives

India is pursuing the tag of "trustworthy outsourcing" with a fierce determination. BangaloreIT.Com, an IT summit which was held in November 2004, focused on outsourcing and issues related to privacy and data security. It is organized by the Department of IT, Biotechnology and Science and Technology in association with Software Technology Parks of India, Bangaluru. The event saw 400 companies from India and 14 other countries participate. International business experts, companies, and IT professionals educated the participants on key issues like best management practices in outsourcing, wireless technology, third-generation technology and information security among other things.

India as a Trustworthy Outsourcing Destination

The proactive measures the Government and individual companies taken have definitely made an impression. Hill & Associates, an enterprise security and risk management consultancy firm, conducted a study which revealed that Indian cities Bangaluru, Hyderabad and Mumbai are low risk outsourcing locations. India is not only moving up the value chain by offering more complex services, but is determined to establish its credibility as a trustworthy destination for outsourcing.

INTRODUCTION

The organizational success rests on the management and protection of the mission-critical data. Data, the essential asset of your business, is extensively used for customer relationship management that includes up-selling, cross-selling and other business services targeted at the customers. Hence, safeguarding business data is vital as its inappropriate usage can lead to greater concerns; this is where Data Security plays an important role.

There is a valid fear that this sensitive information could be altered or used to create negative consequences. Though, Data Security can ensure primary security concerns, it is not the foolproof solution to assure confidentiality. Data Privacy addresses all the issues. It enables sharing of data without compromising its confidentiality.

UNDERSTANDING DATA SECURITY

THREATS TO ORGANIZATIONAL DATA

Protecting customer data has emerged as key issue for organizations today. As data is subjected to a variety of internal or external threats, organizations need a robust security system that not only protects the data from external intrusions but also from internal threats from charlatan employees.

SOLUTIONS FOR DATA SECURITY

Data security addresses following five aspects:

Aspects of Data.

Security.

Available.

Technological Measures:

Availability Backup Technologies, Cluster Solutions, Anti-virus Solutions and so on.

Authentication:

Passwords, PINs, Tokens, Smartcards and Biometrics Technologies like Finger Scan, Iris Scan and so on.

Access Control Lists (ACL), Directories, Firewalls, and so on.

Confidentiality, Integrity, and Non-repudiation SSL, VPNs, Public Key Infrastructure and so on.

Data security can be gained only through a combination of products and processes. Together, they determine the choice of technologies that should be deployed in a particular business case. The technological measures have to be implemented in combination with monitoring technologies, like Intrusion Detection Technologies, to ensure the security of the data assets.

The following three processes should be considered while selecting the various options for data security:

Risk mitigation;

Risk Monitoring;

Business Continuity Plan: Resumption of business operations in the event of a failure.

A security solution that takes into account all the above processes will be a complete and effective solution.

ESSENTIAL COMPONENTS OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

An Information Security Management System (ISMS) needs to be developed to assure complete data security.

The essential components of an effective Information Security Management System that form the building blocks of a complete data security system are:

Risk Management System - This system consists of processes to identify, mitigate, and manage risks.

Security Policy and Security Procedures - This states the organization's security objectives, security levels, and the type of security that it wishes to achieve. The security policy of the organization will form the basis for implementing the security procedures.

Business Continuity Plan - The security policy is essentially a preventive measure to mitigate risks to data assets. However, in the event of a disaster, the Business Continuity Plan serves as the guiding plan to recover and resume business operations within acceptable time.

UNDERSTANDING DATA PRIVACY

Organizations manage large amount of customer data that could be in the form of:

Customer expenditure patterns as in case of Organizations providing Financial Services.

Customer health data as in case of Health Care Organizations.

Projects executed for customers as in case of companies providing technical expertise and so on.

This data is a strategic business asset as it can be used to provide further services to the customer and build other marketing strategies around this data. Corporations could use this asset for cross selling and sharing it with their business partners. The importance of this strategic business asset can be gauged from the 'Goldfish ruling'.

Customer data essentially belongs to the customer and the right to determine its use and disclosure, therefore, belongs to the customer. Data privacy laws have been exemplified this through the HIPAA Privacy Law in the health care sector and the Gramm-Bleach-Blighly Act in the financial services sector.

Data privacy is the responsible handling of customer data by organizations. Data privacy is further complicated because businesses are becoming more and more e-enabled. Some of the challenges in formulating and implementing data privacy solutions are:

Liability towards business partners for data sharing for the cross-selling purposes.

Multiple Customer Databases and Data Warehouses populate Enterprise Systems leading to problems in access control.

Lack of awareness amongst employees.

Outsourcing of business processes.

Diverse Privacy Laws across various countries.

DATA SECURITY v. DATA PRIVACY

Data security essentially refers to protection of corporate business assets from unauthorized access, misuse, and damage. Implementation of data security measures, therefore, is a corporate business need.

Data privacy refers to the responsible handling of customer data by corporations including its secondary use. Secondary use means data collected for one purpose that is subsequently used for other business purposes, like cross selling, that may or may not be known to the customer or business client.

Responsible handling, thus, includes:

Making the customer aware about the purpose of data collection and limiting the collection of data to only the intended purpose.

Taking consent from the customer for every non-standard use of the customer data.

Giving the customer access to data collected from him or her.

Providing recourse in case of violations.

Ensuring the availability and reliability of customer data and preventing it from unauthorized access.

Corporations cannot maintain the privacy of their customer data without implementing security. Data security, therefore, is one of the building blocks for data privacy.

FIVE FAIR INFORMATION PRACTICES

The five building blocks mentioned in the section above are called the five fair information practices which consist of the following:

Notice and Awareness: Corporations should give customers clear and written details about the usage and the disclosure of the data. Systems with customer data and its usage should be made known. A continuous customer awareness program about the use of collected data will optimize transparency.

Choice and Consent: Choice refers to the right of customers to request restrictions on the uses and disclosures of their data. Consent refers to receiving customer's permission before customer data is used and disclosed.

Access: This refers to customer's rights to use their data. Customers should be able to see and get copies of their records, and request amendments. The challenge for organizations is in determining the extent to which customers should be allowed to amend data and the type of data that can be amended or deleted.

Accountability, Enforcement and Recourse: Organizations should be held accountable for the customer data that they possess and for establishing mechanisms that will ensure compliance to policies and procedures. Organizations should provide for reasonable methods to resolve disputes related to the use of data.

Data Security/Integrity: This refers to a data privacy assurance principle stating that gathered customer data, to the extent necessary, would be complete, current and accurate. Organizations must take reasonable measures to assure customer data's reliability for its intended use, and protect it from loss, misuse, alteration, or destruction.

© Universal law Publishing Co.

SUGGESTED QUESTIONS

Q. 1. Write short notes on:

- (a) Difference between cyber offence and cyber contravention.
- (b) Tampering with computer source documents.
- (c) E-commerce.
- (d) Data Protection.
- (e) WPPT.

Q. 2. "Hacking as a cyber crime is most dangerous to Internet because it affects the credibility of Internet and also challenges the existence of e-commerce". Discuss.

Q. 3. Briefly describe the Process of Domain Name Dispute Resolution Process under the UDRP (Uniform Domain Name Dispute Resolution Policy).

Q. 4. What is cyber-squatting? Explain briefly the mechanism of domain name dispute resolution under the Uniform Domain Name Dispute Resolution Policy (UDRP). Whether the WIPO has universal jurisdiction over domain name dispute? What are the legal principles being formulated by Indian Courts to deal with cyber-squatting?

Q. 5. Explain the provisions of the Prasar Bharati Act, 1990 dealing with the composition, powers and functions of the Board and also examine as to whether they were able to discharge its function impartially?

Q. 6. What is the significance of Digital Signature? Briefly explain the provisions of Information Technology Act, 2000 pertaining to creation and verification of Digital Signature. What are the powers and functions of Certifying Authorities?

Q. 7. Write a short note on Breach of Confidence in the context of Confidential Information?

Q. 8. Briefly explain the role of Certifying Authorities under the I.T. Act, 2000.

Q. 9. Briefly explain the difference between Top Level Domains (TLD's) and Country Code Top Level Domains (CCTLD's).

Q. 10. Briefly explain ICANN. What does it do? And what role it plays in Internet?

Q. 11. What constitutes Confidential Information? How is implied confidence established? What are the essentials to prove breach and what remedies are available?

Q. 12. What are the Public Key and Private Key encryption?

Q. 13. The use of Mobile phones for trade, commerce and personal use is getting more and more popular with the development of mobile world. It provides many advantages to common man. Explain.

Q. 14. What is M-commerce about? Also briefly explain its payment mechanism.

Q. 15. What are the stipulations under section 72 with regards to privacy and confidentiality? Explain with relevant case laws.

Q. 16. Briefly explain the two main technologies of Mobile phones.

Q. 17. Explain briefly the Review of Cable Television Act. Its main features, functions and compositions.

Q. 18. Explain the statutory comparison between Handwritten Signatures and Digital Signatures.

Q. 19. Write a note on applicability and non-applicability of I.T., Act, 2000.

Q. 20. Briefly explain the two main parts of payment mechanisms i.e., offline payment system and on-line payment system.

Q. 21. Write short notes on:

(a)Credit Cards and Debit Cards.

(b)E-wallet.

(c)Smart Cards.

(d)SPG (Secured Payment Gateway).

(e)SSL (Secure Socket Layer).

Q. 22. Explain the significance of the Biological Diversity Act, 2002. Briefly explain the functions, powers and composition of National Biodiversity Authority.

Q. 23. Write a Short Note on Biodiversity Management Committees and Local Biodiversity Fund.

Q. 24. Briefly explain the Registration in Bad faith with relevant case laws.

Q. 25. Define Trademark? What are the rights of a Trademark owner? What is Trademark Infringement? Also explain Passing Off Action.

© Universal law Publishing Co.

Table of Cases

Asian paints (India) Ltd. v. Domain Administration, Case No. D 2002-0649	73
Bennett Coleman and Co. Ltd. v. Steven S. Lalwani, Case No. D 2000-0014	72
Castrol Ltd. v. Shrinivas Ganediwal	73
Kharak Singh v. State of Uttar Pradesh, MANU/SC/0085/1962 : AIR 1963 SC 1295: 1963 (2) Cr LJ 329	53
Konkan Railway Corporation Ltd. v. Rani Construction Private Ltd., MANU/SC/0053/2002 : (2002) 2 SCC 388	32
Mahindra and Mahindra Ltd. v. Neoplanet Solutions, Case No. D 2000-0248	73
Mahindra Corporation v. Amit Mehrotra	73
Miler v. California, 413 US 15	49
PUCL v. Union of India, MANU/SC/0149/1997 : (1997) 1 SCC 301: AIR 1997 SC 568	53
R. Rajagopal v. State of Tamil Nadu, MANU/SC/0056/1995 : (1994) 6 SCC 632: AIR 1995 SC 264	53
Ranjit D. Udeshi v. State of Maharashtra, (1965) 1 SCR 6556: AIR 1965 SC 881	49
Reddy's Laboratories Ltd. (Dr.) v. Manu Kosuri, 2001 (3) Raj 122	74
Samaresh Bose v. Amal Mitra, AIR 1986 SC 967: 1986 Cr LJ 24	49
Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd., MANU/SC/0462/2004 : (2004) 6 SCC 145: AIR 2004 SC 3540	74
Tata Sons Ltd. v. Advance Information Technology Association, Case No. D 2000-0049	73
Yahoo Inc. v. Akash Arora, 1999 ALR 620	73

© Universal law Publishing Co.