IT and Cyber Laws

Course Designer and Acquisition Editor

Centre for Information Technology and Engineering

Manonmaniam Sundaranar University

Tirunelveli

IT and Cyber Laws

CONTENTS

Processing of Statistical Data
Accuracy and Timorousness of Data
Data Security
Legal Requirements or Advice
Disclosure to the data subjects etc
Preventing Injury
The Exceptions in Perspective
Data Matching
Codes of Practice
Codes under the Directive

Lecture 6 Data Protection

Transborder Transnational Data Flows (TBDFS)
National controls over Transborder data flows
Establishing conformity with the conventions requirements
Transfer to another convention state
Transfer to nonsignatory state
Transborder data flows and the directive

Lecture 7 **Information Technology Copyright**

Provider liability for user Misuse
Newsgroup postings and copyright
Copyright and WWW pages
Significant legal Issues
Cable programmes and the WWW
Copyright in headlines
Copyright law in Canada

Lecture 8 Nature of Copyright Protection

Right to copyright owner
Substantial Similarity
Literal and non-literal copying
Justifiable similarities
Unconscious Copying
Willful Ignorance
Fair Dealing
Error correction
Back up copies
Reverse Engineering and de-compilation
Reverse Engineering and computer programmers
Other Infringing Acts
Issue of copies to the public
Public Performance
Adaptation and translation
Moral Rights
Resale and rental of copies of a protected work
Computer programmes as audio or visual works
Digital sampling

Computer programmes as photographs or films
IRP in software: An Indian Perspective
How to be copyright protected
Legal action

Lecture 9 **Surveillance Through Information Technology**

Privacy and Surveillance
Forms of Surveillance
The Impact of Technology
Surveillance in the 1990s
Consequences of Data Surveillance
The Legal Response to Data Surveillance

Lecture 10 Individual Rights and Remedies

Implementing Subject Access
Enforced Subject Access
Access Procedures
Providing Access
Examination mark
The extend of access
Data relating to children
Persons suffering mental disorder
Exceptions to the right of access
Law enforcement and taxation
Health Data
Social work data
Judicial appointments

Lecture 11 Legal Privilege

Regulation of financial services
Credit Reference Agencies
Information otherwise available to the public
Order of secretary of state
Failure to provide access
Matters arising subsequent to access
Rectification of inaccurate data
Compensation for inaccuracy
Compensation for unauthorized disclosure
Complaints to the registrar
Subject access in perspective

Lecture 12 Introduction to E-Commerce Law

Meaning of Electronic Commerce
Business to Business E-commerce
Business to customer E-commerce
Benefits of E-Commerce
Risk of E-commerce
Cyber Laws

Initiatives in India
Electronic commerce and the World Trade Organisation (WTO)
The Opportunities of Company Secretaries
The Challenges of the Information Era Digitalization
Communication
Disaggreagating
Impact on Business

Lecture 13 Trade Marks and Service Marks

Patient
Trade Secrets
Cyber Space and Cyber Laws
Issues and Recent Trends in Cyber Laws
The role of ICSI
Emergence of Global E-commerce
Types of E-Commerce
Issues
Cyber Laws
The Electronic Commerce Transaction
Creating a Binding Commitment
Functional Equivalence

Lecture 14 Sources of Law

Validity and Enforceability of Agreements
Offer and Acceptance
Consideration
Statutes of Frauds
Performance
Compliance
Breach
Enforcement
Liability and damages
Evidence
Notice and conspicuousness
Consumer issues
Personal Jurisdiction
Negotiability
Intellectual Property
Illegal bargains and Criminal Law
Dealing with Legal Uncertainties
Legislation and regulation

Lecture 15 UN Model Law on Electronic Commerce

Electronic Funds Transfer Act and Regulation
Digital Signature Legislation
Guidelines

Forms of Agreements
Trading Partner Agreements
Value-Added Network Agreements
Interconnection Agreements
Payments Agreements
Security provision in model agreements
Business Model
The Formalistic Model
The Risk-based Model
Analysis of the Models
Business controls in a Digital Environment
Legal Issues: Indian scenario
Policy Guidelines
Conclusion
Digital Signature
Recent Laws on E-commerce in U.K
Dotcoms, get the Legal Thing Right or Legit to the Court
Business Model
Legal Minefields for Dotcoms

Lecture 16 **Introduction to Cyber Crime and the Law**

The Legal response to Computer hacking
The Computer Misuse Act
The Concept of Access
Limits of authority
Knowledge that access is unauthorized
The ulterior intent offence
The impossible dream
Application of the Ulterior Intent Offence
Unauthorized Modification of data
Logic Bombs
Computer Viruses
The Legal Response
Modification in the Computer Misuse Act
Operation of the Unauthorized modification offence
Hackers sites
Safety on the internet

Lecture 17 The Information Technology Act

The Information Technology Act 2000
Preliminary
Definition

Lecture 18 Digital Signature

Authentication of Electronic Records
Electronic Governance

Attribution, acknowledgement and dispatch of electronic records
Acknowledgement of Receipt
Time and place of dispatch and receipt of electronic records
Secures Electronic records and secure Digital signatures
Digital Signature Certificates
Suspension of digital signature certificate
Revocation of digital signature certificate
Notice of suspension of Revocation
Duties of subscribers
Control of Private Key

Lecture 19 Electronic Signatures

Retention of Electronic Records
Liability of network service providers
Liability of network service providers
Electronic contracts Effectiveness between parties
Attribution
Acknowledgement of receipt
Time and place of dispatch and receipt
Secure Electronic Record
Secure Electronic Signature
Presumption relating to secure electronic records and signature
For the purpose of this section
Effect of Digital Signatures
Presumption regarding certificates
Unreliable digital signature
Reliance on certificates foreseeable
Prerequisites to publication of certificates
Publication for fraudulent purpose
False or Unauthorized request

Lecture 20 Electronic Signatures

Functions of controller
Recognition of foreign Certifying authorities
Controller to act as a repository
License to issue digital signature certificates
Application for License
Renewal of License
Rejection of License
Suspension of License
Notice of suspension of revocation of License
Power to Investigate Contravention
Access to computers and data
Display of License
Surrender of License
Disclosure
Secure Electronic record with digital certificates
Secure Digital certificate
Presumption regarding certificates
Unreliable digital signature

Reliance on Certificate Foreseeable
Prerequisites to publication of certificate
Publication for fraudulent purpose
False or unauthorized request
Duties of certification authorities
- Trustworthy system
- Disclosure
- Issuing of Certificate
- Representation upon Issuance of Certificate
- Suspension of certificate
- Revocation of certificate

Notice of suspension
Notice of Revocation
Duties of subscriber
- Generating Key pair
- Obtaining certificate
- Acceptance of certificate

Control of Private Key
Initiating suspension or revocation
Appointment of controller and other officer
Regulation of Certification authorities
Recognition of foreign certification authority
- Recommended reliance limit
- Liability limits for licensed certification authorities
- Regulation of repositories

Government use of electronic records and signature
- Acceptance of electronic filing and issue of documents
- Obligation of Confidentiality
- Offence by body corporate
- Authorised officer

Controller may give direction for compliance
- Power to investigate
- Access to computers and data
- Obstruction or authorized officer
- Production of documents, data etc

General Penalties
- Sanction of Public prosecutor
- Jurisdiction of Courts
- Composition of offences

Power to exempt
- Regulations
- Saving and transitionals
- Related amendments to interpretation act
- Related amendment to evidence act

Lecture 27 US Administration Statement of Commercial Encryption & Cryptography Policy

The measures the Administration is Considering include
US Cryptography Policy
Key Management and Recovery
Export Controls
Cracking Coded Messages

Lecture 2

Information Legal Practices

Objectives

In this lecture you will be able to

- Know the concept of legal practice
- Describe the committee on data protection
- Know how the European union had played a peripheral role in the data protection arena.

Coverage Plan

Lecture 2

2.1 Snap shot

2.2 International Scenario United Kingdom (U.K)

2.3 The committee on data protection

2.4 About the European Union

2.5 Short summary

2.6 Brain Storm

2.1 Snap Shot - Introduction

A variety of concerns at the potential use and misuse of computers spawned a growing call for legislative intervention. Two general approaches can be identified. The first, as applied within the united states, adopts a sectoral approach with a range of privacy protection statutes being enacted to regulate specific forms of information handling.

A different approach has prevailed within Europe where the tendency has been to enact omnibus data protection statutes. The term 'data protection' made its first appearance in legislation in 1970 and, although it has been criticized as conveying the impression that the information rather than its subjects is to be protected, the phrase has been widely copied. With the passage of the data protection act in 1984 the united kingdom joined the ranks of those states which have legislated in this area. Data protection act revised in 1998 operative from 1 march, 2000.

While it is not intended to present an exhaustive survey of the historical development of data protection legislation in general and the background to the united kingdom data protection act in particular, many of the aspects of current legislation can be understood only in terms of their historical context. This chapter will present an account of the major factors prompting both the introduction and the format of legislation. In this regard account must be taken both of national and of international pressures.

2.2 International Scenario United Kingdom (U.K.)

It is important to mention that a data surveillance bill was introduced unsuccessfully by Kenneth baker mp in 1969. The first significant initiative was undoubtedly the report of the committee on privacy which was published in 1972, chaired by sir Kenneth younger, the committee was established consequential upon the withdrawal of a private member's bill introduced by brian walden mp seeking to establish a statutory right to privacy. The committee's statement was to:

> "consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons or by companies and to make recommendations."

Despite, two attempts by the committee to persuade the home office to extend its statement to the pubic sector, the committee's statement remained restricted to the private sector.

The Report of the Committee on Privacy

In its report, the committee devoted a chapter to the implications of the computer. After receiving evidence as to the nature and scale of processing activities it concluded that 'we cannot on the evidence before us conclude that the computer as used in the private sector is at present a threat to privacy'. Despite this, the committee identified the computer's capability to store and process large amount of personal information, to develop personal profiles and to allow remote access to databases as factors causing legitimate public concern. In order to prevent potential dangers from becoming real, ten data protection principles were formulated which it was recommended should be observed by users on a voluntary basis.

The Ten data Protection Principles :

- Information should: be regarded as held for a specific purpose and not be used, without appropriate authorization, for other purposes.
- Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
- The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
- In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
- There should be arrangements whereby the subject could be told about the information held concerning him.
- The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.
- A monitoring system should be provided to facilitate the detection of any violation of the security system.
- In the design of information systems, periods should be specified beyond which the information should not be retained.
- Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
- Care should be taken in coding value judgments.

The notion that generalized statements of acceptable practice should be incorporated in legislation is one which has been widely accepted in European data protection statutes, although there has also been a developing recognition of the need for the principles to be interpreted in the context of particular forms of data processing. The committee next considered the need to establish machinery to ensure the observance of the above principles. The possibility of introducing a system of self-regulation was considered but rejected as impractical in view of the scale and diversity of computer applications. Perhaps with an eye to the wider usage of computers, the committee recommended that the matter be kept under review and, specifically, that:

> The government should legislate to provide itself with machinery for keeping under review the growth in and techniques of gathering personal information and processing it with the help of computers. Such machinery should take the form of an independent body with members drawn from both the computer world and outside.

The committee's report was published in July 1972. Its contents and recommendations were debated in the house of commons one year later, in July 1973. Speaking in this debate, the home secretary studiously avoided expressing any views on the younger proposals on computers but announced the publication, later that year, of a white paper describing computer practices in the public sector and outlining the government's response to the younger recommendations.

In fact, setting a precedent which was to become depressingly familiar, the white paper, entitled 'computers and privacy', was not published until some two and a half years later, in December 1975. As announced, the white paper's coverage extended into the public sector with a supplement detailing the extent of government computer usage. Whilst the white paper reiterated the finding of the younger committee that there was little concrete evidence of computer abuse, its conclusion was rather different.

The potential dangers were considered so substantial that: 'in the government's view the time has come when those who use computers to handle personal information can no longer remain the sole judges of whether their own systems adequately safeguard privacy.' having announced the intention to legislate in the field of data protection, the white paper indicated that legislation should have two principal components.

First, it would lay down standards and objectives to be met by those handling personal information. In determining the content of these it was suggested that the principles suggested by the younger committee would serve as the 'starting point'. Subsequent government actions moved the report of the younger committee to the finishing post.

Second, moving beyond the recommendations of the younger committee, machinery should be provided to ensure compliance with the statutory requirements. It was further recognized that the topic was a novel one, that statements of general principles would require considerable extension and specification. Accordingly, it was announced that a data protection committee was to be established with a statement to make detailed recommendations as to the scope and extent of data protection legislation and as to the form of supervisory mechanism which should be introduced.

2.3 The Committee on Data Protection

With hindsight, the publication of the white paper can be seen as marking a high-water point in governmental enthusiasm for the concept of data protection. This enthusiasm was certainly matched by that of the data protection committee which, under the chairmanship of Sir Norman Lindop, presented its voluminous report in June 1978. This remains the most comprehensive and detailed survey of the impact of data processing activities upon the rights and liberties of the individual conducted in the united kingdom. It proposed that a multi-member data protection authority should be established. Anyone using a computer to handle personal information would be obliged to register details of their activities with this authority which would also be charged with ensuring compliance with seven data protection principles. These should be divided into three categories, designed to safeguard the interests of individuals, of those holding information and, finally, the wider interests of society.

In terms of their content these principles are not dissimilar from those advocated by the younger committee. Noteworthy, however, is the grouping of the principles into three categories; those designed to safeguard the interests of those who handle data, its subjects and, more novel, those of society as a whole. Such an approach provides explicit recognition of the validity of the various claims and interests involved in this area and attempts to provide a framework for the resolution of any conflicting claims.

Recognizing the 'nebulous nature of these broad statements of principle, the committee recommended that they should be supplemented by the creation of a number, estimated at around 50, of statutory codes of practice targeted at and providing detailed provisions relating to, particular users or categories of user. The report of the Lindop committee received a lukewarm governmental reception.

In march 1981, in response to a parliamentary question as to the government's intentions, the home secretary announced that: 'the government has decided in principle to introduce legislation for this purpose when an opportunity occurs.' the report of the committee on data protection was largely ignored and in particular the home secretary announced that instead of establishing an independent data protection authority, responsibility for the operation of the data protection regime would be vested in the home office. This element of the government's response produced considerable criticism, with skeptical commentators expressing doubts as to whether the home office, which enjoys at least a measure of responsibility for some of the most sensitive computerized informational practices involving the police and national security agencies, could constitute a satisfactory public guardian against any abuse emanating from these quarters.

Following a further round of consultations, a further white paper was published April 1982. By this time the lindop report was reduced to the status of 'very helpful background information'. In one fundamental respect, however, the government view had changed. Following sustained criticism of its proposal that the home office should operate the registration scheme, the need for independent supervision of data users was recognized. The lindop suggestion of a multi-member data protection authority was not, however, accepted; instead it was proposed to appoint a single data protection registrar.

Enactment of the Data Protection act

A data protection bill based on the provisions of the white paper was introduced in the house of lords in November 1982. It successfully passed through this house but fell at the committee stage in the house of commons when parliament was dissolved prior to the 1983 general election. An amended SIII was speedily introduced by the incoming government, receiving the royal assent on 12 July of the Orwell Ian year, 1984.

Although the act's parliamentary passage produced some heated debate, conducted largely although not exclusively on party political lines, these centered on particular issues rather

than on the general concepts. The timetable behind the legislation, with proposals extending through the life-span of four governments, would appear to indicate that the subject enjoyed a low priority on the agenda of the major political parties.

The fact that the 1984 act is not radically dissimilar to kennetla baker's 1969 bill must be a cause for some concern. Fifteen years of computer development appear to have made little impact on the legislature's consciousness and, as will be discussed in the following chapters, many of the act's concepts could be considered obsolete or inappropriate even as it reached the statute book.

In commanding the first data protection bill to the house of commons the home secretary commented that it was designed 'to meet public concern, to bring us into step with Europe and to protect our international, commercial and trading interests'. While undoubtedly civil libertarian concerns are fundamental to the concept of data protection it is significant that these represented only one out of five interests identified and that, at least numerically, commercial and trading factors assumed greater significance. One reason for this can be seen in a letter to 'the times' from a leading industrialist arguing that;

> Lack of computer privacy legislation may seriously affect our overseas trade. Of the nine ace countries only Italy, Ireland and the united kingdom have no laws or firm legislative programme. Britain is regarded as becoming a 'pirate offshore data haven' by countries that have legislated on computer privacy.

Continuous concern was expressed at the possibility that privacy considerations might serve as a smokescreen for the imposition of data sanctions against the auk.

> "it is difficult to distinguish between private and commercial data when it is being transmitted between countries. It would be all too easy for foreign data inspection boards to forbid export or import of data ostensibly to protect its citizens' privacy but in reality to protect employment or revenue by restricting trade with Britain."

The validity of this observation is demonstrated by several well documented instances in which British companies had been prevented from carrying out data processing or related activities on behalf of Swedish companies owing to the Swedish authorities' concern at the lack of legislative safeguards.

Even prior to the first national interventions, pressure had been exerted for international action in this field. In addition to a concern over the extent to which the application of computer technology could serve to threaten human rights, the justification for the

intervention of international agencies was seen as being two fold. First, it was recognized that given the scale of the international trade in computerized information impossible burdens could be placed upon multinational enterprises should they be required to comply with differing standards in every country in which they acquired, stored, processed or even transferred data.

A second factor lies in the realization that, in the information age, national boundaries have become almost redundant. One nations efforts to protect its citizens' liberties balancing restrictions upon the forms of data processing that may be carried out, could easily be nullified were the data to be transferred abroad for processing. From the standpoint of data users it would not be surprising were undertakings to seek to base their processing in that country or those countries whose laws placed the fewest restrictions on their activities, i.e. Who were willing to provide a data haven. It has, for example, been reported that a 'diversified consumer products company rented a house which straddled the border of two European countries to maintain the option of having computer tapes in the venue most expedient to management purposes'.

Fear of the establishment of data havens undoubtedly prompted much international action in this field and, as will be discussed, the issue of the control of transponder data flows has proved to be one of the most controversial aspects of the directive. During the 1970s and 1980s most of the international initiatives in the data protection field were pursued within the council of Europe and the organization for economic cooperation and development. The following sections will consider the major activities carried out under the auspices of these organizations.

Brief attention will also be paid to the work of the united nations. During the 1990s much of the focus has switched to work within the European union and the slow progress towards the adoption of the 'directive of 24 October 1995 on the protection of individuals, with regard to the processing of personal data and on the free movement of such data'. The substantive provisions of this instrument will receive detailed consideration in the following chapters. In the present chapter an account will be given of the forces prompting community involvement in the field and the progress to legislation.

The Council of Europe

In 1968 the parliamentary assembly of the council of europe addressed a request to the committee of ministers that they consider the extent to which the provisions of the european convention on human rights safeguarded the individual against the abuse of modem technology. The assembly noted particular concern at the fact that the european convention, together with its united nations predecessor, the universal declaration of human. Rights, had been devised before the development and widespread application of the computer. The committee of ministers passed this request to its committee of experts on human rights, which in 1970 reported the view that the protection offered under existing conventions was inadequate. In particular it was pointed out that the european convention and similar documents were based largely on the premise that individuals' rights might be infringed by the actions of public authorities.

The development of the computer placed a significant weapon in the hands of private agencies. Whilst identifying the dangers of computer abuse, the committee's report also drew attention to a paradox which remains unresolved to this day. Data protection seeks to give an individual a greater measure of control over personal information and to place controls over the dissemination of this information. This approach may conflict with another individual's claim to be allowed access to information under the european convention on human rights.

Here it is provided that everyone has the right to freedom of expression. This shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'. The issue is similar to that discussed above relating to the exercise and extent of the right of privacy. In 1986 the parliamentary assembly of the council of europe approved a recommendation on data protection and freedom of information. This advocated that the committee of experts on data protection be instructed 'to identify criteria and principles according to which data protection and access to official information could be reconciled'.

Although data protection and freedom of information are. Not inherently opposed in that both concepts seek to improve the position of individuals against those organizations which hold information of relevance to aspects of their life, to date, no action has been taken under this recommendation. Acting upon the committee's report, two separate resolutions were adopted by the committee of ministers dealing with the private and the public sectors. The differences between the two sets of recommendations are comparatively minor and for both sectors it was recommended that national laws should ensure that:

- The information stored should be accurate and kept up to date. In general information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

- The information should be appropriate and relevant with regard to the purpose for which it has been stored.

- The information should not be obtained by fraudulent or unfair means.

- Rules should be laid down or specify the periods beyond which certain categories of information should no longer be kept or used.

- Without appropriate authorization, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

- As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

- Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

- Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of mis-directions of information, whether intentional or not.

- Access to the information should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

- Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.

The initial council of europe resolutions did not attempt to prescribe the means by which member states should give effect to the principles contained therein. As more and more countries enacted data protection legislation during the 1970s so the problems resulting from the international trade of information, frequently referred in other states.

In its preamble the convention reaffirms the council of europe's commitment to freedom of information regardless of frontiers and proceeds explicitly to prohibit the erection of national barriers to information flow on the pretext of protecting individual privacy. This prohibition extends, however, only where the information is to be transferred to another signatory state. Impliedly, therefore, the convention permits the imposition of sanctions against any non-signatory state whose domestic law contains inadequate provision regulating the computerized processing of personal data. A recalcitrant state could effectively be placed in data quarantine.

The council of Europe's activities in the field of data protection have not ceased with the entry into force of the convention. A substantial number of recommendations have been addressed to member states concerning the interpretation and application of the convention principles in particular sectors and in respect of particular forms of processing. Table one gives details of these instruments.

Table 2.1 : Council of Europe recommendations

Title recommendation (81)1	Regulations for automated medical data banks
Title recommendation (81)19	Access to information held by public authorities
Title recommendation (83)3	Protection of users of computerized legal information services
Title recommendation (83)10	Protection of personal data used for scientific research and statistics
Title recommendation (85)20	Protection of personal data used for the purposes of direct marketing
Title recommendation (86)1	Protection of personal data used for the social security purposes
Title recommendation (87)15	Regulating the use of personal data in

	the police sector
Title recommendation (89)2	And other related operations
Title recommendation (90)19	Protection of personal data used for payment and other related operations
Title recommendation (91)10	Communication to third parties of personal data held by public bodies
Title recommendation 1037(1986)	On data protection and (1986) freedom of information

It will be noted that the involvement of the council of Europe has diminished since 1991, a time scale which parallels the EU's increasing interest in the topic.

The Organization for Economic Cooperation and Development (OECD)

Although the convention provides that the committee of ministers may invite any state not a member of the council of europe to accede to this convention, no external states have attempted to exercise this option. The work of the council of europe has been viewed with considerable suspicion by a number of countries including the united states.

The difference in regulatory philosophy between the United States' sectoral and, the European omnibus approach has been identified above. In one respect statutes such as the Privacy Act of 1974, the Fair Credit Reporting Act of 1970 and state legislation such as the Californian Information practices

Act of 1977 offer wider protection to the individual as legislation typically applies to all records coming within a specified category regardless of whether the information is held on computer or in manual form. Against this, the individual's rights are dependent upon whether a law has been promulgated in a particular area.

Faced with this divergence of approach the view has been expressed by several American commentators that the provisions of the convention were motivated more by considerations of commercial expediency and economic protectionism than by a genuine concern for individual privacy. In the course of a meeting of the committee of experts, the united states observer contrasted the sectoral approach adopted in that country with the omnibus data protection legislation envisaged under the convention, and concluded that:

> The draft convention appears to regulate a function, that is, it appears to regulate automated or electronic data processing and what the automated data processing industry might do with records about individuals. To our mind the draft convention is, in essence, a scheme for the regulation of computer communications technology as it may be applied to personal data record-keeping. The establishment and exercise of individual rights and the privacy of the individual seem to be treated in a secondary fashion . . . I would note particularly that the word 'privacy' is rarely mentioned in the convention and is not included in its title.

The difference in approach between the council of europe and the aced approaches has been explained in terms of the differences in approach existing between the civil and common law systems of law. Thus it has been stated that :

> In the final result, although substantially similar in core principles, the convention and the guidelines could be analogized, albeit in a rough fashion, to the civil and common law approaches, respectively. Common law systems proceed pragmatically formulating the rules of legal behavior as they acquire experience, while the civil law tradition tends to rely upon, codification of rules in advance of action.

Although a representative of the united states was afford observer status at the meetings of the council of Europe's committee of experts, its major input in this area, has been through its involvement in the activities of the OECD. This organization's efforts in the field, o£ data protection parallel those of the council of Europe, and in 1980 the council of the OECD agreed 'Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data' (hereafter the guidelines'). As approved; the Guidelines are broadly in line with proposals submitted by the united states delegation. At first glance the scope of the guidelines appears wider than that of the convention. The latter applies only in the situation where personal information is subjected to automatic processing whilst the former are to:

> Apply to personal data; whether in the public or the' private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

Despite this discrepancy insofar as substantive provisions are concerned, there is a considerable degree of overlap between the convention and the guidelines. Almost invariably, however the particular provisions of the guidelines are less precise than their equivalents in the convention. Thus, in relation to the question o£ transparency of data processing, the convention provides that :

> Any person shall be enabled . . . To establish the existence of an automated data personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.

Whilst the guidelines merely advocate that:

> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

A further declaration on Transporter data flows was adopted by the OECD in April 1985. This made reference to the fact that:

> Flows of computerized data and information are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of member countries, these flows acquire an international dimension.

and indicated its signatories intention to :-

- Promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;
- Seek transparency in regulations and policies relating to information, computer and communications services affecting trans border data flows;
- Develop common approaches for dealing with issues related to trans border data flows and when appropriate, develop harmonized solutions.
- Consider possible implications for other countries when dealing with issues related to Transporter data flows.

It is clear from these objectives that commercial and trading interests provide at least as significant a force for action as do concerns for individual rights. Although the declaration commits its member countries to conduct further work relating to specific types of Transporter data flows, especially those accompanying international trade, marketed computer services and computerized information services and intra-corporate data flows, no further measures have been adopted.

The United Nations

On 20 February 1990, the united nations economic and social council agreed 'guidelines concerning computerized personal data files'. These identify ten principles which, it is stated, represent the 'minimum guarantees that should be provided in national legislation'. The principles follow what might be regarded as the standard model but there are two features of these guidelines which justify mention at this point.

First, they make provision for the application of the principles by international agencies, bodies which might fall outside national laws. Second, the united nations guidelines provide the option for the extension of the principles both to manual files and to files held concerning legal persons.

2.4 The European Union

Until the early 1990s the european union had played a peripheral role in the data protection arena. This could be ascribed to two main causes. First, the limited nature of the legislative competencies conferred by the establishing treaties gave rise to doubts whether and to what extent the european community was empowered to act in this field.

Although the increasing importance of information as a commodity within the single market has provided a basis for european action, the exclusion of matters coming within the ambit of national security and, to a partial extent, criminal and taxation policy, has served to limit the scope of the european union's intervention. A second factor influencing work in this field had been a reluctance on the part of the commission to duplicate work being conducted under the auspices of the council of europe. In 1979 the european parliament's legal affairs committee published a report 'on community activities to be undertaken or continued with a view to safeguarding the rights of the individual in the face of developing technical progress in the field of automatic data processing'. In it the committee recognized both the dangers to individual privacy resulting from computer data bases and also the implications of divergent national provisions for the community's competition policy and for the creation of a common market in data processing.

It accordingly proposed that a community directive be prepared 'on the harmonization of legislation on data protection to provide citizens of the community with the maximum protection'. In the parliamentary debate which followed the publication of this report the

commission representative expressed his sympathy with the motives behind the proposals but argued that no community action should be taken until there was a clearer indication of progress at the council of europe. In 1981 the commission addressed a recommendation to member states that they sign and ratify the convention.

By 1990 the convention had been signed by all the community member states but ratified only by six. As will be described, the convention affords considerable discretion to signatories regarding the manner in which they comply with their obligations. The instrument also establishes minimum standards.

A number of member states had enacted laws which were considerably in advance of the convention's minimum standards whilst others such as the united kingdom had openly indicated an intention to do the bare minimum necessary to satisfy obligations under that instrument. By 1990, commission concern at the effect discrepancies in the member states' laws and regulations might have on inter-community trade resulted in proposals being brought forward for a directive 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data'. The objective of the proposal was stated to be to harmonize the data protection laws of the member states at a 'high level'.

The community legislation, it was further stated, would 'give substance to and amplify' the provisions of the convention. The commission proposal for a general directive in the area of data protection was accompanied by a further proposal for a directive 'concerning the protection of personal data and privacy in the context of public digital telecommunications networks'.

The proposed telecommunication privacy directive fell foul of the post-masticate doctrine of 'subsidiarity' and was withdrawn for reconsideration. A revised version has reached the stage of a common position being adopted but it is unclear whether or when the legislation will finally be adopted. Following a five-year journey through the european union's legislative process, the data protection directive was adopted on October 24, 1995 and requires to be implemented within the member states by October 1998. The very right of the to legislate in the data protection held has not gone unchallenged. The directive invokes the authority of article 100a of the treaty which empowers harmonization measures where this is necessary for the attainment of the single market.

The argument effectively is that the maintenance of different standards of data protection within the member states constitutes an impediment to the free movement of data. Reliance upon article 100a has a further significant consequence in that any harmonizing measures introduced under its authority have to secure a high level of protection. Effectively, therefore, the directive has to secure a level of protection equivalent to the highest currently available in the member states. It is unclear how effective the directive has been in this regard with complaints being aired from countries such as Germany that implementation might dilute their existing regimes, especially in respect of trans border data flows. For the united kingdom, implementation of the directive will require significant changes to existing united kingdom law.

In particular, the home office expressed an initial preference for implementing the requirements of the directive by statutory instrument under the authority of the european communities act 1972. Although such an approach would have the benefit of enabling the speedy introduction of the required changes, such legislation is limited to matters falling within the competence of the eu. The preamble to the directive recognizes that:

> Whereas the activities referred to in titles v and vi of the treaty on european union regarding public safety, defense, state security or the activities of the state in the area of criminal laws fall outside the scope of community law, without prejudice to the obligations incumbent upon member states under article 56(2), article 57 or article 100a of the treaty establishing the european community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the state does not fall within the scope of this directive where such processing relates to state security matters;

Significant aspects of the data protection act 1984 concern activities coming under these headings, in particular where the processing activities of the police or inland revenue are concerned. These would have remained subject to the 1984 regime while other forms of activity would have been subject to the new regulatory schema. Responses to the home office consultation paper indicated a strong preference for the introduction of new primary legislation and, perhaps influenced also by a change of government, the intent to proceed on this basis was announced in the queen's speech in June 1997. A further paper, 'data protection. The government's proposals' was published in august 1997.

Domestic scenario

The computers were introduced in a big way in India by late Sh. Rajiv Gandhi accordingly number of policies were framed such as talcum policy, internet policy. However, legislation on terms of computer/information technology is still awaited. The union government on l6th December, 1999 introduced in the lok sabha a bill called the information technology bill which has been passed on l7th may, 2000. This law has adopted the model law on electronic commerce adopted by the united commission on international trade law and it aims at amending the Indian penal code, the Indian evidence act, 1872, the banker's book evidence act, 1891, and reserve bank of India act, 1934 and for matters connected there with or incidental there to. The exempt of the act is given at the and of this book.

2.5 Short Summary

- Data Protection Principles were formulated to prevent potential dangers.
- The publication of white paper can be seen as marking a high water point in governmental enthusiasm for the concept of data protection.
- Britain is regarded as becoming a pirate offshore data haven by countries that have legislated on computer privacy.
- A recalcitrant state could effectively be placed in data quarantine.
- The draft convention is appeared to regulate automated or electronic data processing.
- Flow of Computerized data and information are increasing the economic status. It acquires an international dimension.

2.6 Brain Storm

- Explain the Committee on privacy.
- Give note on principles data protection.
- Discuss about the enactment of the data protection act.

- How the Organization for Economic Co-operation and Development (OECD) working?
- Role of European Union in Data Protection.

Lecture 3

Theft of Information

Objectives

In this lecture you will be able to

- Know the property rights in information
- Know about dishonest exploitation of confidential information

Coverage Plan

Lecture 3

3.1 Snap Shot – The basis of the offence of theft

3.2 Property rights in information

3.3 Borrowing as theft

3.4 Dishonest exploitation of confidential information

3.5 Information Theft in Japan

3.6 Short Summary

3.7 Brain Storm

3.1 Snap Shot - The basis of the offence of theft

According to Oxford dictionary theft could be defined as "dishonest appropriation of another's property with intent to deprive him or her of it permanently. A variety of definitions can be found in the works of the institutional writers. Hume, for example, defines it as encompassing 'the felonious taking and carrying away of the property of another'. In England, the offence of theft has a statutory basis, with the Theft Act 1968 providing that a person will be guilty of theft where he dishonestly appropriates the property of another with the intention of permanently depriving the owner of that property.

According to Oxford dictionary property is referred as something owned, a house, Lord, money etc. 'Property' is defined as including 'money and all other property, real or personal, including things in action and other incorporeal property'. In the case of information, two objections lie to the relevance of a charge of theft. First, unless the information is held on some storage device which is also removed, it is difficult to see how the Scottish requirement of 'taking and carrying away' or the English requirement of depriving the owner of property can be satisfied. With recognized forms of theft, the conduct has two elements.

The owner loses possession of the property and the thief acquires possession. Unlike the situation where, for example, a car is stolen, possession of the information will not be lost. It is possible that this objection could be countered with the proposition that the holder has lost exclusive possession or knowledge of the information, but even if this argument were to be accepted and it could clearly apply only to information that was in some way confidential a second objection relates to the question of whether information might be regarded as property for the purpose of the law of theft During parliamentary debate on the Theft Act it was suggested that the statutory definition of 'property' would encompass the theft of a trade secret. Such an interpretation, however, does not appear compatible with the decision of the Divisional Court in the case of Oxford v Moss.

3.2 Property rights in information

Moss was a student at Liverpool University. In a manner unfortunately not disclosed in the Law Report, he discovered and surreptitiously removed a proof copy of an examination paper which he was due to sit. His plan was to copy the contents of the paper and, being aware that it the paper were discovered to be missing, a replacement paper would be set, to

return the paper to its original location. Upon his conduct being discovered, the question arose as to whether any criminal offence had been committed. As it was an integral part of his scheme that the original paper should be returned, it was considered that he could not be charged with the theft of the paper.

A prosecution was brought, however, alleging theft of the confidential information contained in the paper. Moss was acquitted by the Liverpool magistrates on the basis that confidential information could not be regarded as property. This conclusion was upheld by the Divisional Court, which declared that whilst the holder of information might possess limited rights in it which could be upheld at civil law, the information itself was not property and hence could not be stolen.

An example of the distinction between rights in and property rights over information can be taken from the decision of the House of Lords in the case of Rank Film Distributors Ltd. v Video Information Center. In the course of civil proceedings involving an allegation of breach of copyright the appellants sought discovery of a variety of documents in the possession of the respondents. In resisting this application, the latter claimed that disclosure would expose them to the risk of criminal proceedings for, inter alia, theft of the appellants' copyright interests and, therefore, would infringe their privilege against self-incrimination. This prospect was dismissed by Lord Fraser, who commented:

> The risk of prosecution under the Theft Act 1968 may, I think, be disregarded as remote, because that Act applies to theft of 'property' which is defined in a way which does not appear to include copyright but only, so far as this appeal is concerned, to the physical objects such as tapes and cassettes which are of small value by themselves.

In the 1988 Copyright, Designs and Patents Act it is now provided that copyright 'is a property right which subsists in accordance with this Part in the following descriptions of work ….

Despite this apparent grant of property status, it would appear that the rights conferred under the copyright legislation are exhaustively defined therein. In the case of Paterson Zucchinis v Merfarken Packaging Ltd. Oliver LJ sitting in the Court of Appeal dismissed an allegation that the respondents owed a common law duty of care to avoid actions which might result in an infringement of the appellants' copyright interests, holding that :

> the plaintiffs' case ultimately depends upon the existence, alongside the statutory duty not to infringe copyright, of a parallel common law duty owed to the copyright owner to take

> reasonable care not to infringe copyright. For my part I am wholly unable to accept the existence of such an additional or parallel duty

Such a conclusion is in conformity with the principles of intellectual property law, which constitutes an exception to the general rules against acts restricting competition. As such, the extent of copyright protection is to be found in the copyright legislation. A number of cases within the United States have held that information can be the subject matter of theft.

In the case of United States v Girard and Lambert, for example, the Court of Appeals for the Second Circuit interpreted a statutory prohibition against the unauthorized sale of any 'record . . . or thing of value' as encompassing the unauthorized abstraction and sale of information. Given the different definitions applied to the subject matter of theft, it is doubtful whether consideration of United States precedents assists significantly in the consideration of the United Kingdom situation.

Stewart attempted to obtain details of the names and addresses of hotel employees. This information was sought by a trade union which wished to recruit members from amongst these employees. The information was contained in personnel files held on the employer's computer. Stewart's scheme was to persuade an employee to copy the data from the computer without, however, removing any tangible objects.

The scheme being discovered, Stewart was charged with the offence of counseling the offence of theft 'to wit: to steal information, the property of the . . . Hotel contrary to s 283 of the Criminal Code'. This provides that :

> Everyone commits theft who fraudulently or without colour of right takes, or fraudulently and without colour of right converts to his use or the use of another person, anything whether an inmate or inanimate. . .

Although the word 'anything' appears in the above provision, all the courts dealing with the case were agreed that the word had to be interpreted in the sense of any 'property'.

At trial, Stewart was acquitted by the judge (Krever) who held that information, even confidential information, could not be regarded as property :

> …confidential information is not property for the purpose of the law of theft in Canada... If this interpretation should be thought to be inadequate to meet the needs of modern Canadian

> society, particularly because of its implications for the computer age, the remedy must be a change in the law by Parliament. It is not for a court to stretch the language used in a statute dealing with the criminal law, to solve problems outside the contemplation of the statute. If an accused person's conduct does not fall within the language used by Parliament, no matter how reprehensible it might be, it ought not to be characterized as criminal.

This, view was supported by Lacourciere JA in the Court of Appeal but the majority were in favour of conferring at least a limited property status upon confidential information, Houlden JA stating;

> While clearly not all information is property, I see no reason why confidential information which has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purpose of its business should not be regarded as property and hence entitled to the Protection of the criminal law.

The Court of Appeal decision was subjected to considerable criticism and ultimately was overturned in the Supreme Court on grounds similar to those adopted by Krever J. Thus it was held that should it be determined that the protection of the law of theft should be extended to confidential information, this was a decision for Parliament. It was also pointed out that there were competing interests involved in the free flow of information and in the right to confidentiality.

In its Consultative Memorandum, the Scottish Law Commission concluded that information could not be the subject of theft under Scots law. It quoted with approval the words of the Canadian House of Commons Standing Committee on Justice and Legal Affairs, which had argued :

> For reasons of public policy the exclusive ownership of information which, of necessity, would flow from the concept of 'property', is not favoured in our socio legal system. Information is regarded as too valuable a commodity to have its ownership vest exclusively in any particular individual.

The Scottish Law Commission concluded that questions of the status of information and as to whether certain forms of dealing W it should be subject to criminal sanctions raised wide issues of policy that extended beyond the computer field. For this reason, and taking account of the problems previously identified in applying the law of theft to information, no recommendation was made for change in this area.

The same approach was adopted by the Law Commission whose working paper makes the point that :

> the definition of property for the law of theft, and the argument as to whether it is possible to appropriate information belonging to another with the intention of permanently depriving the other of it are problems which have general implications outside the region of computer misuse.

This view is in line with the earlier findings of the 4Vorking Paper on Conspiracy to Defraud. Here, whilst affirming that 'information, particularly confidential information, will often be regarded as a valuable commodity. Information of one kind or another is frequently bought and sold', the view was taken that the authorities referred to in this chapter established that it could not possess. a sufficient property status to constitute the subject matter of theft.

3.3 Borrowing as Theft

The question as to whether a temporary removal of objects will constitute a criminal offence is one which considerably predates the computer age. The issues involved are however, especially relevant in this context. Given the ease and speed with which large amounts of data stored on a computer storage device may be copied, a party may obtain benefit equivalent to that normally obtained through theft by means of a temporary removal. Consideration of the situation under both Scots and English law suggests that different conclusions regarding the criminality of such conduct might well be reached north and south of the border. As an example in English Law.

Borrowing in English Law

An example of a situation which may be regarded as typical of the ‘borrowing' scenario can be found in the English case of R v Lloyd. This case involved an alleged conspiracy to remove copies of feature films from cinemas overnight with the intention that they should be used to produce video copies for resale. As has previously been stated, the English law of theft has traditionally required evidence of an intention permanently to deprive the owner of his property The Theft Act 1968 did, however, introduce a new provision to the effect that :

A person appropriating property belonging to another without meaning the other permanently to lose the thing is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose

of regardless of the other's rights; and a borrowing or lending of it may amount to so treating it if, but only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal.

Charges brought under this section were dismissed by the Court of Appeal, which adopted an extremely restrictive interpretation of its scope. The first part of the section, it was held, would apply in situations where the taker's conduct amounted to blackmail. The second part, which was at issue in the present case, would be applicable only where the taker's intention was to return the item only when all of its value had been extracted.

In the present case the Chief justice held that this criterion had not been satisfied as 'The goodness, the virtue, the practical value of the films to the owner had not gone out of the article. The film could still be projected to paying audiences'. On the basis of this case it would appear that a temporary appropriation will constitute theft only if the intention is to return the item only when it is worthless.

A situation such as that at issue in the present case, where the value of the film might be considered to have been reduced because those persons who obtained video copies might not pay to see the film in a cinema, will not suffice. In the computer context, if a disk were to be removed and copied with the original subsequently being deleted prior to its return, this might suffice to constitute theft but the mere acts of borrowing, copying and returning will not.

3.4 Dishonest Exploitation of Confidential Information

Issues similar to those described above were discussed in the recent Scottish case of Grant v Allan. The appellant Grant was employed by a firm of carriers. In the course of his employment it was alleged that he did 'clandestinely take and without lawful right or authority, given by your said employers or otherwise, detain copies of a quantity of . . . computer printouts' .

It was common ground between the parties that the word 'take' was to be interpreted in the sense of causing a computer to make the printouts rather than in that of removing printouts which had already been made: The printouts detailed the employers' customers and it was alleged that Grant offered to sell these to a competitor. A meeting was arranged for this purpose.

The competitor subsequently reported the approach to the police and Grant was arrested when he sought to keep the appointment. Before the Sheriff a plea was taken to the relevancy of the charge. This was rejected but an appeal was brought before the High Court. The debate here centered on two issues: first whether the conduct complained of constituted a crime under the law of Scotland and second, on the assumption that the conduct was not currently illegal, whether the High Court should exercise its historic declaratory power to 'punish every act which is obviously of a criminal nature'.

In arguing that the complaint leveled against Grant was one recognized under Scots Law, the Advocate Depute made reference to a variety of authorities including two dating back to the seventeenth and eighteenth centuries. The case of Dewar has been referred to above. Here the defender was an apprentice to a printing company.

The proprietors of the company made use of a variety of formulae in mixing printing ink. This information was regarded as confidential and details were recorded in books. which were normally kept under lock and key. Wishing to obtain details of the formulae, Dewar broke into the room where the books were kept, `carried them away, got them copied, and afterwards replaced them in the situation from which they had been taken'. Although no full report of the case exists, Burnett reports that the court held the Dewar had committed a punishable act. In the event despite the Advocate Depute's argument that the talking and retaining of the books constituted the mechanics' rather than the 'essence' of the crime which, he contended, lay with the unlawful dealing in the information the court rejected the argument that Dezvar was authority for the 'proposition that the law of Scotland recognizes as a crime the dishonest exploitation of the confidential information of another'. Rather, it was concluded, the unlawful means by which Dewar had obtained the books constituted the basis of the conviction.

The authority which appeared most relevant to the present case was that of HM Advocate v Mackenzie. The defender in this case was charged with two offences, first stealing a book of chemical recipes belonging to his employer and, second, with making copies of the recipes with intent to dispose of them for profit in breach of an agreement of secrecy with his employer.

This second charge was dismissed by the Lord Justice Clerk (Macdonald) who held that 'I am quite unable to hold that this is a relevant charge of crime, either completed crime or attempted crime'. The point will again be relevant in considering the provisions of the

Computer Misuse Act. Essentially, it was considered that Mackenzie's scheme had not progressed sufficiently far to constitute a criminal attempt.

Having found that the conduct libeled was not the subject of an existing offence, the court considered whether it should exercise its declaratory power to make it so. Such a suggestion was unanimously condemned by the court. Both the Lord Justice Clerk and Lord Wylie quoted a further passage from Lord Salvesen's judgment in Mackenzie to the effect that the second charge sheets forth a breach of the accused's contract of service with his employers, but this is primarily a civil wrong'.

Such a proposition was also held relevant in Grarzt v Allan. The conduct, it was held, was not so clearly of a criminal nature that it should be so declared. Conctxrring, Lord Macdonald concluded:

> To make a declaratory finding that it is a crime dishonestly to exploit confidential information belonging to another would have far reaching consequences in this technological age. If it is felt that the sanction of the criminal 1aw is required to prohibit such a practice this should be introduced by legislation and not by the declaratory power of the High Court.

Although the doctrine of the High Court's declaratory power applies only in Scots law, the case and the discussion serves to illustrate the limits of legitimate judicial creativity

3.5 Information Theft in Japan

Case – 1

A computer software engineer was arrested on suspicion of stealing client information from a Tokyo Bank and selling Tokyo data base administrator. The administrator was also arrested the next day. The engineer was working free lance for Sakura Bank from where he copied the information (personal details) of 20,000 clients onto a floppy disc and sold it for 200,000 yen. Yasunori Fujisama, 34, was developing client Management software for the Sakura Bank at the time of the theft the administrator of Personal File Library, 73 year old T. Tamura, was arrested after he tried to sell the information to Sakura Bank.

Source : "Arrest in Sakura Bank Data Theft", Asah : evening News (News paper, Japan) 8 January, 1998. 2nd Arrest in Data Theft", Asah : evening News, (News paper, Japan) 19 January 1998.

Case – 2

Police were asked to bring charges against a 35 year old employee of a Osaka based art dealer, after it was learned that she had sold all of their client and prospective client information data information companies in Tokyo and Osaka. The company, a dealer in Japanese wood block prints has excess of 530,U00 people; this information has been collected over a period of 6 years and included names, address etc. There were also credit card information and art preference of 18,000 customers. It is one of the largest breaches of privacy ever recorded, of the 100 plus employees, the woman was one of only that had access to the data base. Her employer discovered that she had ordered a copy of the disc from the company that had organized the information on magnetic-optical disc. She retired shortly after. She is believed to have received more than 5 million yen (approximately $45,40,000) for information she had passed on.

Source : "Osaka art trader sold out art lovers". (Asah : Evening News, (News paper, Japan), 26 January, 1998).

3.6 Short Summary

- According to Oxford dictionary theft could be defined as "dishonest appropriation of another's property with intent to deprive him or her of it permanently"
- The risk of prosecution under the Theft Act 1968 applies to theft of physical objects such as tapes and cassettes.
- Copyright is a property right according to the copyright, designs and Patents Act of 1988.
- Information particularly confidential information will often be regarded as a valuable commodity was the findings of the 4v working paper on conspiracy to defraud.

3.7 Brain Storm

- Explain the role of the property rights in Information.
- Explain the Information Theft cases in Japan.
- Whether borrowing is a theft. Explain with examples.

Lecture 4

Scope of Data Protection

Objectives

In this lecture you will be able to

- Know the concept of processing
- Describe the data protection actors
- Know the compliance with the council of Europe convention
- Describe the Breaches of Security or Protection

Coverage Plan

Lecture 4

4.1 Snap Shot

4.2 Manual Records and Data Protection

4.3 Concept of Processing

4.4 Personal Data

4.5 Distinguishing opinions form intentions

4.6 Computer bureau/processors

4.7 Exceptions to the legislation

4.8 National security and data protection

4.9 Compliance with the council of Europe convention

4.10 Breaches of Security of Protection

4.11 Short summary

4.12 Brain Storm

4.1 Snap shot

Despite a ready identification of the prime target, neither the Act nor the Directive essay any definition of the word 'computer'. The word, indeed, is not mentioned at all in the Directive and is referred to in the Act only in the context of the operation of a 'computer bureau'. The reluctance to attempt a definition is common to virtually all statutory interventions in this area. The British Data Protection Act 1984 applies in respect of 'equipment operating automatically in response to instructions given for that purpose`, modified and ratified in 1998 and operative from 1st March 2000. Whilst the Directive refers to `the processing of personal data wholly or partly by automated means'.

Certainly, these definitions will apply to every known form of computer, but are also capable of applying to a variety of other forms of equipment. Many homes and offices possess a telephone directory of the form whereby details of individuals and their telephone numbers are recorded on cards with each letter of the alphabet being allocated one card. A series of keys on the front of the equipment correspond to the letters of the alphabet. Pressing any key will cause the directory to open at the relevant page. It might be argued that such an activity involves automated processing.

More serious definitional problems may arise with certain forms of microfiche devices. Where the filmed records are linked with some form of computerized index, so that the selection by a user of an entry serves automatically to cause the relevant screen of text to be displayed, it seems clear that the system will fall under the ambit of the legislation. These instances may be expected to constitute the exception rather than the rule, and for the sake of simplicity, references will be made throughout this chapter to computers and to computerized records.

4.2 Manual Records and Data Protection

One of the key areas of distinction between the Act and the Directive is in respect of their treatment of manual records. These are totally excluded from the provisions of the Act. This is in accord with the Convention's requirements, although provision is made for its signatories to give notice that they will 'also apply this Convention to personal data files which are not processed automatically. The total exclusion of paper-based records presently leaves open the possibility that data users may maintain the bulk of their record's-consisting of non-controversial data on computer but withdraw sensitive items to a small manual file,

retaining a linking reference on the computer. In this way, the user retains much of the benefit of automated processing whilst avoiding the controls and safeguards associated with data protection legislation.

The Directive's approach is very different. By referring to data being processed 'wholly or partly by automatic means', the manual elements of hybrid systems of the kind referred to above will be brought within its ambit. More significantly, the Directive will apply to certain forms of manual records. The Preamble states that the justification for this is:

> Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2(c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

Whilst Article 2 provides that the legislation is to apply to:

> . . . the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

Although it is clear that some manual records will be included in the new data protection regime, it is unclear how extensive this will be. The Data Protection Registrar has commented that those states which currently make provision for the inclusion of manual records have interpreted the requirement in a restrictive fashion and the Government has indicated a preference for a similar approach to cover:

> . . . card indexes, microfiches and similar collections from which personal data are capable of being readily extracted. It would also include files about named individuals in which each item has an internal structure conforming to some common system. An example might be a file with the subject's name or another unique personal identifier on the cover and containing one or more proformas.

The extension of the legislation to manual records was one of the most controversial aspects of the Directive, with United Kingdom opponents estimating the compliance costs to industry at some £100 million for the banking sector alone. It should be noted, however, that the Consumer Credit Act 1974 and the Access to Health Records Act 1990 provide for access to credit and medical records irrespective of the format in which these are stored, whilst the Local Government (Access to Information) Act, 1985 and the Open Government Code of Practice provide extensive rights of access to information. As the Data Protection Registrar has commented:

> Experience elsewhere indicates that in practice, in many cases, information provided in response to Freedom of Information requests will relate to the individual making the request.

Given that the keepers of manual records will likely be exempted from the notification requirements and also the expressed intent to restrict the application of the legislation to structured files, it is difficult to see how estimates of vast additional cost are likely to be fulfilled-even if there should be a massive increase in the present numbers of requests for subject access. Given that access rights may be the most important issue for most individuals, restriction to the most structured forms of manual records may not be a matter of great concern.

The Directive additionally provides an extensive transitional period of twelve years although this applies only to files in existence at the date of the Directive's adoption, Even in this limited situation, the subject access and rectification provisions of the Directive, must apply from the date of the introduction of national implementing statutes.

4.3 The Concept of Processing

The two key requirements for the application of data protection legislation are that there should be processing and that this should relate to personal data. Under the Data Protection Act, 1984, processing is defined as encompassing the acts of:

> *. . . amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of these operations by reference to the data subject.*

The Directive's definition is considerably broader, referring to:

> . . . any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

In terms of the activities involved, adoption of the Directive's approach should close the loophole created by the decision of the House of Lords in the case of R v Brvzun. Here, a police officer had caused data relating to individuals to be displayed on a terminal attached to the police national computer. Beyond being seen and noted, it was not alleged that any further use had been made of the data.

The defendant was charged under the Data Protection Act, 1984 with the wrongful use of data contrary to the provisions of section 5 of the Act and was convicted at trial. Overturning the convictions, the House of Lords held by a majority that a distinction had to be drawn between the activities of processing and of use. As was stated by Lord Hoffmann:

> In my view, however, the scheme of the Act as a whole does not permit the phrase 'use [personal] data' to be constructed as including its retrieval. This is because the Act quite carefully uses a number of different words to describe various things which can be done to personal data. These include holding, using, disclosing, transferring, obtaining and, for present purposes most in significantly, 'processing'.

Accepting that the defendants' activities constituted processing, the question was posed whether it also amounted to using the data? Lord Hoffmann continued:

> I do not think that it can. The Act treats processing differently from using . . . So it seems to me that 'using personal data was not intended to include the various operations within the computer which fall within the definition of Processing'.

The concept of 'use', it was concluded, had to be interpreted in line with the normal meaning of the word and would require that some action be taken on the data. The consequence is that unfair or even unlawful processing of data will not constitute a criminal offence under the Act in the absence of evidence that some further use is made of the data. The broader definition adopted under the Directive will bring together the concepts of processing and use.

The Act contains a further requirement that data should be processed by reference to a data subject. The application of this provision has been unclear. It might be, for example, that a university will have on computer a list of the names of all the students attending a particular

class together with the marks which each obtained in exams. If the data is processed so as to compile a list of all students obtaining a mark of 60% or above, it is clear that data has been extracted, but has it been extracted by reference to individuals? This point assumes considerable importance in relation to direct mail where the goal of the processing may be to produce a list of potential customers.

The Data Protection Registrar has expressed the view that this form of activity will constitute processing conducted by reference to every individual whose details are involved, but the issue has not been tested before the courts. The Directive omits the requirement that data be processed by reference to a data subject, referring to 'any operation or set of operations which is performed upon personal data'. A further problem which may remain under the Directive concerns the definition of the word 'recorded'. For the purposes of the Data Protection Act 1984 the word 'data' is defined as:

> . . . information recorded in a form in which it can be processed automatically in response to instructions given for that purpose.

The Directive does not provide a separate definition of 'data' but its definition of 'Processing' cited above makes reference to the act of recording data. The question when information is recorded may b-e a matter of some difficulty. In the case of R v Gold, the House of Lords held that the word 'recorded' required the preservation of the thing which is the subject matter of them for an appreciable period of time with the object of subsequent retrieval or recovery'. As the Data Protection Registrar has commented, many modern computer systems require that data be held in the system for only a short period of time. The development of the Internet and WWW means that the availability of access to data is becoming an acceptable substitute for its possession. In R v Gold, for example, the particular data was retained for less than one second.

The issue may assume considerable importance where data is being transferred from one user to another. Direct communications between computers may allow large amounts of data to be transmitted and received in a very short period of time. Once again, the issue might more properly be considered as one of control rather than the strict application of the legislation.

4.4 Personal Data

Not all data will be classed as personal data and it has been estimated personal data accounts for only some 2%-5% of all data which is subject to automated processing. The bulk of the data concerns financial matters or relates to the activities of companies or other legal bodies. The Data Protection Act 1984 applies where processing takes place of:

> ….information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expressions of opinion about the individual, but not any indication of the intentions of the data user in respect of that individual.

While the Directive refers to the processing of :

> . . . any information relating to an iden6fied or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physchological, mental, economic, cultural or social identity.

Two issues arise concerning the implementation of the Directive. Under the Act there is a specific restriction to data concerning living individuals. The Directive makes no mention of this topic and the Registrar has suggested that there might be instances where it would. be justifiable to extend the scope of the legislation. One situation postulated is where a deceased person left clear instructions that information was not to be published. It would appear, however, that the Government is minded to retain the restriction. Under the Act the decision whether an individual is identifiable has to be made by reference to information available to the data user.

Clearly, where the data is directly linked to the name of an individual this criterion will be satisfied. The Act provides that the individual may be identified from the personal data held and from `other information in the possession of the data user'. This other information need not be held on computer. An example of the application of this provision might be seen in the case of a computer system which is designed to log telephone calls. It is likely that the record will indicate only the instrument from which the call emanated together with details of the destination and duration of the call.

No reference will be made to any individual but possession of a telephone directory will enable the person responsible for the call to be identified. Where the data is transferred to a third party, the Data Protection Act 1984 will not regulate the transaction where the additional key necessary to identify data subjects is not also transferred or disclosed.

The Directive's approach is more extensive referring to identification by information or means likely to be used by the data user or by 'any other person'. It may be, for example, that aggregate data on individuals, resulting for example from a census, may make no reference to individuals but that these could be identified by third parties linking the original data with other sources of information in their possession.

Although this approach is to be welcomed as preventing data users colluding so as to evade the legislation by arranging for different users to control data and means of identifying, it will also oblige data controllers to consider what forms of processing may be carried out by third parties. The operator of a web site, for example, may put information on line including stories or reports produced by a particular author.

Assuming no further processing was carried out, it is unlikely that the operator would be regarded as a data user under the existing United Kingdom legislation. It is possible, however; that other web users could, through the application of search engines, conduct searches by reference to the author and by doing so compile a list of on-line publications and citations.

4.5 Distinguishing Opinions from Intentions

One of the most problematic aspects of the Data Protection Act's definition concerns the distinction between expressions of opinions and intentions. Even the Data Protection Registrar has commented to the effect that it is not at all clear what the distinction is between an opinion and an intention' and recommended that the distinction be withdrawn. The justification put forward in Parliament for the exclusion of expressions of the user's intentions towards the data subject was twofold.

First it was stated that intentions are personal to their holder rather than to their subject. This argument has some force, but exactly the same factors apply in respect of opinions.

A more substantial argument is that data relating to intentions often relates to matters such as an employer's plans for the development (or otherwise) of the subject's career. Premature disclosure might be undesirable. The Government have proposed that this matter should be dealt with by providing for exemptions from the subject access right rather than by continuance of the present blanket exclusion.

Data Protection Actors

For the purposes of the Act, the world is divided into three categories:

- Data Users,
- Computer Bureau, and
- Data Subjects.

Although the terminology is somewhat different, the scope of the Directive is broadly equivalent with reference made to :

- Controllers
- Processors and
- Data Subjects.

In respect of the first two categories, the scope of the statutory definitions extend considerably further than might be expected and, in particular, it is not necessary that a person own or operate any form of computer equipment in order to come within the regulatory schema. It has been indicated that the United Kingdom will adopt the Directive's terminology in introducing enabling legislation.

Data user/controller

Under the Data Protection Act, 1984, a data user is defined as a person who holds data. A person holds data if:

> . . . the data form part of a collection of data processed or intended to be processed by or on behalf of that person . . . and
>
> . . . that person (either alone or jointly or in common with other persons) controls the contents and use of the data comprised in the collection; and
> the data are in the form in which they have been or are intended to be processed . . . or (though not for the time being in that form) in a form into which they have been converted after being so processed and with a view to being further so processed on a subsequent occasion.

The Directive uses the term controller A controller is defined as:

> . . . the natural or legal person, public authority, agency o other body which alone or jointly with others determines the purposes and means of the processing of personal data.

It is to be noted that with both Act and Directive, the test for inclusion in this category relates to the control of data rather than the actual act of processing. It is quite possible for persons to be classed as data users or controllers even though they do not own a computer. An example might concern the owner of a small business who records details of transactions on pieces of paper which are stored in the archetypal shoe box. Once a year the shoe box may be collected by an accountant who transfers the data to computer in order to prepare a set of accounts.

Assuming that some of the data in the accounts relate to individual creditors and debtors, all the criteria necessary for the application of the legislation will be satisfied and, doubtless much to their surprise, the business person will be classed as a data user/controller. In such a situation the accountant will also be so regarded, the Divisional Court confirming in the case of Data

Protection Registrar v Griffin that anyone who processed data on behalf of clients would be regarded as a data user when he or she possessed any control or discretion concerning the manner in which the processing was carried out.

A similar situation is postulated in the Directive :

> . . . where a message containing personal data is transmitted by means of a telecommunications of electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.

4.6 Computer bureau/processors

A computer bureau is operated by any person who:

> . . . pro*cesses data on behalf of a third party-whether on a regular or an occasio*nal basis-or allows them to use his equipment for that purpose.

Whilst a processor is :

a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Once again, these two terms appear broadly equivalent although the Act's definition may be somewhat broader in its application to the situation where permission is given for the use of equipment. The inclusion of the word 'occasional' in the phrase 'whether on a regular or an occasional basis' is significant. The owners of two small businesses occupying adjacent premises might discover, for example, that both use the same sort of computer.

The phrase 'I don't know how we could manage without it' might trip lightly from their mouths. In these circumstances, it would be very natural for them to reach an agreement so that in the event of one computer suffering a breakdown, its owner would be allowed to use the neighboring machine. As soon as this agreement is implemented, the party whose equipment is utilized will fall to be regarded as operating a computer bureau.

Although both parties may be aware that they are data users, the fact that they are also to be regarded as operating a computer bureau, or acting as a data processor, may come as an unwelcome surprise. A further query has been raised concerning the Directive whether an employee who carries out processing might be classed as a processor. The better view would appear to be that the term is restricted to the activities of third parties.

It may also be the case that with the proliferation of microcomputers in the workplace, equipment may be used by employees for purposes unconnected with their employment. In the event that these involve the processing of personal data the employees in question will be classed as data users/ controllers. If the employer explicitly or tacitly permits these activities, the employer will be required to register as operating a computer bureau.

The concept of a data subject poses few problems. A data subject is an individual who is the subject of personal data.

4.7 Exceptions to the legislation

The breadth of the definitions discussed above coupled with the vast numbers of computers in use today ensures that data protection laws will apply to a vast range of computer-related activities. Some 3.5 million personal computers were sold in the UK alone during 1995. To this figure must be added other information technology-based devices such as telephones or fax machines which contain the facility to store frequently-used numbers so as to allow abbreviated dialing. It might not be unreasonable to estimate that 20 million inhabitants of the United Kingdom might possess equipment which is at least potentially capable of bringing them into the category of data users or processors.

Individuals become data users only when they process personal data. Those who use computers purely in order to play games are unlikely ever to come within this category. Even so, the numbers involved are potentially huge. The exclusion from the scope of data protection legislation of those data users perceived as operating on a small scale or whose activities pose no perceptible threat to the individual constitutes a major feature of the United Kingdom legislation. Such an approach is sanctioned by the Council of Europe Convention which provides for signatory states to give notice that they:

> . . . will not apply this convention to certain categories of automated personal data files . . . in this list it shall not include, however, categories of automated data files subject under its domestic la w to data protection provisions.

While the Convention places no formal limits upon the extent to which this provision may be utilized, the fact that a State making use of the above provision may not claim the application of the Convention as against other State in respect of excluded files serves to restrict its practical utility

Treatment of exemptions has been the cause of some uncertainty and controversy under the Data Protection Act. The fundamental problem arose from the decision to adopt a system of universal registration of data users. The merits of the registration system will be considered in more detail below hut under the Act's approach, if a data user is exempted from the requirement to register, it is also exempted from the requirement to comply with substantive requirements such as the grant of subject access. This has resulted in most of the exceptions being tightly drawn, so much so as to prompt comment from the Registrar to the effect that they:

> . . . are likely to apply only to small businesses. Such business might have their own microcomputers or may have work undertaken through a general computer bureau or possibly a professional accountancy firm. More sophisticated users-which will inevitably include the majority of large businesses as well as some small ones will find that the exemption does not apply to them because they are unable to observe the conditions as to use and disclosure of the data.

Exemptions under the data protection act

At present the following exemptions are offered under the Data Protection Act :

- Information which is required by law to be made available to the public, e.g. the electoral roll or lists of company shareholders.

- Data held by unincorporated Members' Clubs for membersh5p purposes where members have not objected to the processing of their data.

- Mailing lists where all those whose details are held have consented to the processing.

- Payroll and Accounting Data so long as the data is not used for any other purpose, e.g. assessing the credit rating of a customer.

- Data held only for the management of personal, family or household affairs.

Exemptions in the directive

A rather different approach is adopted in the Directive. This provides that it is not to apply where processing takes place :

- In the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense State security (including the economic well being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

4.8 National security and data protection

The treatment of data processed for purposes connected with national security has been a controversial aspect of the United Kingdom system and will be considered in more detail below. Although the decision to implement the Directive by means of primary legislation opened the way to reform of all aspects of the legislation, the Government have indicated that there is to be no change in the provisions relating to national security.

In respect of the raft of minor and technical applications exempted under the Data Protection Act, there seems no doubt that with the exception of processing for domestic purposes, these will be brought within the regulatory structure. Unlike the Act, however, the Directive contains provision for such applications to be exempted from the requirement of notification (registration) whilst retaining the obligation to conform with the substantive requirements of the legislation.

Given that much of the criticism of the present legislation has centered upon the bureaucratic nature of the registration process, this might well extend the coverage of the legislation at marginal cost to the data users affected. Indeed, as will be discussed, the Directive's implementation may offer the opportunity for radical simplification of the registration process to the benefit of large numbers of data users. Many aspects of data protection require the striking of a balance between competing interests.

The argument in favour of exempting data held for the purpose of safeguarding national security can be simply put. Data protection attempts to ensure openness and accountability in respect of data processing. Some forms of processing are, however, so closely linked to the vital interests of the state that they require to be undertaken away from the public gaze. In these situations the arguments in favour of secrecy outweigh those of transparency. This claim may be most strongly advanced where the activities in question impinge upon questions of national security.

Although the Directive excludes national security from its area of coverage, the United Kingdom legislation is also intended to comply with the provisions of the Council of Europe Convention. This instrument recognizes that certain categories of processing should not be subjected to the full rig ours of a data protection regime providing that:

Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

Although the Convention provides for special treatment to be afforded to a variety of informational practices, chiefly lying within the public sector, it is only in respect of information held for the purposes of national security that the United Kingdom legislation totally excludes the application of the Data Protection Act. In respect of the other areas of activity the Act provides for limited or partial exemption from some of its provisions, in particular those relating to subject access.

As will be discussed, this provision is capable of excluding very many data processing activities from the ambit of the legislation. In analyzing these matters, consideration may be conducted under two headings, the first concerning its scope within the UK legislation and the second assessing the conformity of the UK approach with the requirements of the Convention.

National security in the data protection act

The Act essays no definition of the scope of national security. This is in line with the practice of governments throughout the years. The traditional response of prime ministers faced with a parliamentary question seeking explanation as to the scope of national security interests has been on the lines:

This term has been in general use for many years in a variety of contexts and is generally understood to refer to the safeguarding of the state and the community against threats to their survival or well being. I am not aware that any previous Administration has thought it appropriate to adopt a specific definition of the terrti.

It has recently been reported that every telex message sent from the United Kingdom is routinely scanned by the security services. Under the Data Protection Act provisions any government minister is empowered to certify conclusively that any holding of personal data is done for the purpose of safeguarding national security. In such event, the provisions of the Data protection Act will have no application. The breadth of this provision is in direct conflict with the recommendation of the Linden Committee that any use of this power should be carried out by the Home Secretary as the Minister primarily responsible for internal security

A further cause for concern follows from the fact that certificates to this effect will be issued only subsequent to the activities of a data user being challenged by the Data Protection Registrar or before the courts. Processing of personal data by the elusive national security agencies will not be the subject of any form of notification to the Registrar unless or until some form of challenge arises.

Whilst the nature of the activities of national security agencies often requires that their operations be shrouded in a deal of secrecy the UK appears unusual in the extent to which this principle is applied. The Lindop, Committee recommended that whilst the subject access provisions should not extend to information held by a national security agency and, whilst details of the informational practices of these bodies would not appear on the Data Protection Register, it should be ensured that:

> . . . the DPA has at least one senior official with a security clearance sufficiently high for him to be able to operate in effect as a privacy consultant to the Home Office and the security services, and to work out with them the appropriate rules and safeguards or their systems.

There would appear to be no compelling reason why a similar approach should not be adopted in the United Kingdom and, indeed, a similar system has been introduced under the interception of Communications Act 1985. Here, an independent Commissioner has been appointed to monitor the operation of the system of authorizing interceptions introduced by the legislation. A Tribunal is also established which is empowered to investigate complaints from individuals who consider that their communications have been subjected to unjustified interceptions.

4.9 Compliance with the council of Europe Convention

The compatibility of the Data Protection Act's treatment of national security with the Convention's requirements may be queried in two significant respects: first, whether the approach of totally excluding this sector of data processing can be classed as a 'derogation' from the general provisions, and second, whether the approach adopted constitutes a 'necessary measure in a democratic society'.

The Convention sanctions 'derogation' from its provisions An its normal dictionary sense, the word refers to a partial repeal or abrogation of a law. Such terminology would appear more

consistent with the limitation of the application of data protection legislation within specified circumstances rather than its complete exemption or exclusion. This interpretation is supported by the fact that in a number of cases concerning the application of the European Convention on Human Rights which utilizes the same terminology, the European Commission and Court of Human Rights have refused to accept that a total withdrawal of Convention rights can be justified by recourse to the dictates of national security.

In this context it is relevant to give further consideration to the background to the Interception of Communications Act. The introduction of this statute was required following the decision of the European Court of Human Rights in the case of Malorre v Llnited Kingdom, where it was held that the previous system of authorizing interception of communications was in breach of the European Convention on Human Rights which requires that any interference with the privacy of an individual's correspondence must be:

> ... in accordance with the law and ... necessary in a democratic society in the interests of national security, public safety or the economic well being of the country for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

In the Malone case the Court found against the UK on the narrow ground that interceptions were sanctioned by administrative fiat rather than by any legal provision. No examination was, therefore, required of the substantive aspects of the interception procedures. The extent of the requirement imposed by the Convention was discussed in the earlier case of Klaus v Federal Republic of Germany, in which the defendant state's procedures were subjected to detailed scrutiny. Under the relevant provisions of German law, it was required that an individual who had been subjected to surveillance was to be informed of this fact as soon after its termination as could reasonably be done without prejudicing the purposes of the investigation.

Additionally, all interceptions required to be sanctioned in advance by an independent Commissioner who is appointed by a parliamentary committee, albeit after consultation with the government. Any material obtained through the interception is not to be handled directly by the investigating officers but is submitted first to an official, qualified to hold judicial office, who will pass on only such material as is considered relevant to the purposes of the investigation.

Considering these points, the European Court held that the German system complied with the requirements of the Convention. It recognized the legitimate call for secrecy where national security interests were concerned and that requirements of notification could not be elevated into an inviolate principle, pointing out that:

> The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification of each individual affected by a suspended measure might well jeopardize the long-term purpose that originally prompted the surveillance.

None the less, the Court was riot uncritical of aspects of the German system and it would appear from the judgment that the question of compliance was a finely balanced one. It would certainly appear that a total exclusion of individual rights would not have passed their scrutiny.

Generally the term privacy, integrity and confidentiality are loosely construed to be synonymous with security or protection. These, however, have different connotations with respect to data or information. They also address different areas of information system. To better understand the scope, measures and to ensure protection in each area it is important to look at the definitions of these terms.

1. SECURITY : "The data or information security is the protection of data against accidental or intentional destruction, disclosure or modification." Computer data security refers to the technological safeguards and managerial procedures which can be applied to computer hardware and data to ensure that organizational assets and individual privacy are protected.

2. PRIVACY : Is a concept applied to individual. It is the right of an individual to decide what information he/ she wishes to share with others or is willing to accept from others.

4.10 Breaches of Security or Protection

There are number of manners by which losses of data or information takes place and these are :

i. Theft of PC and Media

ii. Damage due to breakage

iii. Environmental damages

iv. In advert corruption/loss

v. Environmental losses

vi. Malicious damage/leakage

vii. Unauthorized access

viii. Modification Erasures etc.

ix. Computer viruses

x. Data Typing

4.11 Short Summary

- The distinction area of the Act and Directive is their treatment of manual records.
- The extension of legislation to manual records was one of the most controversial aspect of the directive.
- Holding, using, disclosing transferring and obtaining of data is called data processing.
- Information which relates to individual who can be identified from that data is called personnel data.
- Treatment of exemptions has been the cause of some uncertainty and controversy under the Data Protection act.

4.12 Brain Storm

- Discuss about the concept of processing.
- Explain the data protection act.
- Describe briefly the Breaches of Security.
- Give note on personnel data.
- Explain the Exemption under Data Protection Act.

Lecture 5

Data Protection Principles

Objectives

In this lecture you will be able to

- Know the principles the data protection
- Know the exceptions to the nondisclosure principles
- Know how to secure, use store and to process the data

Coverage Plan

Lecture 5

5.1 Snap Shot

5.2 Acquisition of data

5.3 Parties authorised to supply

5.4 Relevancy borough Council

5.5 The Community Charge

5.6 Rhondda Borough Council

5.7 Exceptions to the fair obtaining requirements

5.8 Data protection and the media

5.9 Fair Processing

5.10 Credit scoring

5.11 Caller identification

5.12 Processing of statistical data

5.13 Accuracy and timorousness of data

5.14 Data security

5.15 Legal requirements or advice

5.16 Disclosure to the data subject etc

5.17 Preventing injury

5.18 The exceptions in perspective

5.19 Data matching

5.20 Codes of Practice

5.21 Codes under the directive

5.22 Short Summary

5.23 Brain Storm

5.1 Snap Shot

Whilst notions of the form of supervision of data users have changed significantly over the years, the substantive requirements of acceptable processing practice have remained more stable. The notion of requiring data users to comply with general statements of good practice has been a feature of many data protection instruments. The number of principles has varied but their content remains much the same. Their eight enforceable principle of good practice for personal data processing according to Data Protection Act and there are :

- fairly and lawfully processed;
- processed limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with data subject rights;
- secure; and
- not transferred to countries without adequate protection.

Source : Data Protection Act, Government of U.K. The Stationery Office Limited.

Data Protection Principles

i. The Data Protection Act establishes eight data protection principles requiring data users to ensure that:

ii. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

iii. Personal data shall be held only for one or more specified and lawful purposes.

iv. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

v. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

vi. Personal data shall be accurate and, where necessary, kept up to date.

vii. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

viii. An individual shall be entitled

ix. Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

The Directive also prescribes five 'principles relating to data quality', requiring Member States to ensure that personal data and these are :

i. Processed fairly and lawfully;

ii. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

iii. adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

iv. accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

v. kept in a form which permits identification of data subjects, for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The discrepancy in numbers is explicable by the fact that the broader definition of processing adopted in the Directive has the effect of merging the scope of the first, second and third principles whilst provisions regarding subject access and data security are treated separately in the Directive. The Registrar has suggested that the United Kingdom principles should be recast to take account of the Directive's approach although the number would remain at eight.

The most significant changes would relate to the seventh and the eighth principles where the Directive's provisions are considerably broader than their equivalents in the Act. In many respects, the principles can be considered a data processing equivalent to the ten commandments. Opinions may vary whether it is a mark of technological progress or regress that computers require rather fewer commandments than their human controllers.

As with the commandments, the general formulations of the principles frequently require to be interpreted in the context of particular applications. Whilst few, for example, could object to a requirement that data be obtained fairly, the determination of what is fair can be made only in the context of a particular situation or application. Both Act and Directive provide more detailed guidance regarding a number of the principles, often prescribing exceptions from their application. As with other statutes, further guidance on issues of interpretation has become available through decisions of the courts and the Data Prevention Tribunal resolving actual cases.

Finally, both instruments envisage a significant role for sector specific codes of practice although the legal status of these is rather obscure. The data protection principles cover all aspects of data processing. Although the distinction is blurred by the Directive's broad definition of processing, it may be helpful to consider their operation in relation to various stages of this activity. An obvious starting print is with the manner in which data is acquired. This will then be processed and put to use. Use may take a variety of forms and would include disclosure of data to a third party.

A final function moves the focus from the obligations imposed upon the data user to the rights conferred on the data subject and introduces the concept of subject access.

5.2 Acquisition of Data

The key requirement in both Act and Directive is that information be obtained fairly and lawfully. It may be relatively straightforward to determine whether information has been obtained lawfully, but the criterion of fairness raises more subjective issues.

The act of obtaining is also dealt with in the Directive's second principle which makes reference to the collection of data for 'specified, explicit and legitimate purposes'. An

illustration of the operation of the principle and the concept of ‚subject consent' which is an integral feature of the Directive can be seen in the decision of the Data Protection Tribunal in the case of Innovations (Mail order) Ltd v Data Protection Register.

The appellant operated a mail order business. It solicited custom in a variety of ways including the distribution of catalogues and the placing of advertisements in various media including newspapers, radio and television. Customer orders might be placed either in writing or over the telephone. In order to secure the delivery of goods, it is clearly necessary that customers provide details of their name and address and it was accepted that there was no need specifically to inform them that the information would be used for this purpose.

It was also accepted that customers should realize that their details would be retained by the appellant and used as the basis for future mailings of its catalogues. In addition to using the information to solicit further custom from the individuals concerned, however, the appellant made the information available to other organizations, a practice known as 'list broking'. The appellant's catalogues gave customers notice of this possibility and its order forms offered customers the opportunity to exclude use of their data for broking purposes.

Some adverts, especially those appearing on radio or television, did not make mention of the possibility and in the event that catalogue orders were placed by phone no mention would be .made of this secondary purpose. An acknowledgement of order would, however, be sent and this would convey the message:

> For your information. As a service to our customers we occasionally make our customer lists available to carefully screened companies whose products or services we feel may interest you. If you do not wish to receive such mailings. please send an exact copy of your address label to. . .
> .

The Registrar took the view that notification of the intended use came too late in the contractual process and served an enforcement notice alleging a breach of the first data protection principle and requiring, inter ala that where notice was not given in promotional material, the subject's positive consent must be secured prior to the data being used for list broking purposes. Effectively, therefore, the system would become one of 'opting in' rather than 'opting out'.

A number of arguments were put forward by the applicant as justifying their practices. It was suggested that at the time of placing an order, customers would be concerned primarily with

obtaining the goods and that a notice along the lines referred to above will have limited impact. Where, orders were made by telephone, giving specific notice would increase the length of the call thereby increasing costs for both the supplier and the customer.

It was also pointed out that the details would not be used. for list broking purposes until 30 days from the date the acknowledgement or order was sent. Thus, it was suggested, allowed ample time for the customer to opt out. It was also pointed out that the appellant's practices were in conformity with an industry code of practice and the Council of Europe's Recommendation on the protection of personal data used for the purposes of direct marketing. Notwithstanding these factors, the Tribunal upheld the Registrar's ruling.

Use of the data for list broking purposes, it was held, was not a purpose which would be obvious to the data subjects involved. Fair obtaining required that the subject be told of the non-obvious purpose before the data was obtained.. Whilst a later notification might be a commendable way of providing a further warning', it could not stand by itself. Where prior notification might not be practicable, the Tribunal ruled 'the obligation to obtain the data subject's positive consent for the non-obvious use of their data falls upon the data user'.

The decision of the Tribunal in the Innovation case was affirmed by a differently composed Tribunal in the case of Lingua phone Institute v Data Protection Registrar' Once again, the conduct complained of lay in obtaining information from customers or potential customers enquiring about the appellant's products and services without disclosing at the time of obtaining that the information might also be used for list broking purposes. In view of the decision in Innovation, there was no doubt that this conduct was unlawful. By the time of the Tribunal hearing, the appellant had modified its advertising to include a notice:

The tribunal expressed concern that :

> . . . the opt-out box appears in minute print at the bottom of the order form In the Tribunal's view the position, size of print and wording of the opt-out box do not amount to a sufficient indication that the company intends or may wish to hold, use or disclose that personal data provided at the time of enquiry for the purpose of trading in personal data. The Tribunal relies upon the Data Protection Registrar to agree a wording which should ensure that a proper explanation is given in all future advertisements.

Effectively the Tribunal ruling seeks to ensure the data subject's informed consent at the point w here data are collected. Although the decision is compatible with the Directive's

requirements, this appears to impose even more extensive requirements. Where data is collected from the data subject, it is provided that, save where this is already known, information must be given as to the identity of the controller, the purposes for which the data are intended to be used and any recipients of the data.

Where necessary to ensure that subsequent processing is fair, the subject must also be informed whether providing answers to any questions is voluntary or compulsory and as to the possible consequences of a failure to reply. Notice must also be given of the right of subject access. Where data is obtained from a third party, notice of the factors given above must be supplied at the time the data is recorded or disclosed to a third party.

5.3 Parties authorized to supply

In certain situations, parties may be authorized, or even required, to make information publicly available. The Data protection Act provides that:

Information shall in any event be treated as obtained fairly if it is obtained from a person who

- is authorized by or under any enactment to supply it; or
- is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom;

> and in determining whether information was obtained fairly, there shall be disregarded any disclosure of the information which is authorized or required by or under any enactment or required by any such convention or other instrument as aforesaid.

The provision that information will always be regarded as having been obtained fairly when it is obtained from a person statutorily authorized to supply it assume considerable significance in the case of electoral registers. These constitute perhaps the most comprehensive listing of names and addresses available to data users. Under the terms of the Representation of the People (Amendment) Regulations 1990,1 Electoral Registration Office are obliged to supply copies of the register for their area upon request:

Prior to the introduction of these regulations the Officers were recruited to supply copies of the Register only where these were readily available. The Data Protection Registrar commented, that A number of Officers 'had effectively ceased to supply their registers for use

for other purposes. Following representations from the Data Protection Registrar; the Home Office introduced a scheme whereby a list of those purchasing copies of the Register is maintained by each Officer and made available for public inspection. Although electoral registers may represent the most extensive record of be made available to the public.

Concern has been expressed on a number of occasions at the use made of lists of company shareholders, particularly in the case of privatized undertakings which might have several hundred thousand shareholders. It may be argued that the purpose of making details of shareholders publicly available is to also, identification of the owners of a limited liability company. Use of this information for the purposes of compiling mailing lists for direct marketing purpose raises different issues although it is difficult to see how prohibitions might be enforced against the use of publicly available information for such purposes.

5.4 Relevancy and scale of the Information obtained

The other principle which is pertinent to the acquisition of data is the fourth requiring that data shall be `adequate, relevant and not excessive'. The Directive uses the same term. No further guidance is available in either instrument concerning the application of these requirements. The principle has, however, been at issue before the Data Protection Tribunal in the course of proceedings brought against a number of Community Charge Registration Officers.

5.5 The community charge

The Community Charge or 'poll tax' has proved one of the Most controversial forms of taxation introduced in recent times. Although much of the publicity generated concerned its financial aspects, the implementation of the requirement that registers be established of those liable to pay the tax attracted the attention of the Data Protection Registrar. Compilation of the Community Charge Registers was the responsibility of Community Charge Registration Officers in each local authority area.

Where the intention was that the register should be maintained on computer, an application would require to be submitted for registration under the Data Protection Act. In the case of four applications, submitted by the Registration Officers for, Harrow -Borough- Council,

Runnymede Borough Council Rhondda Borough Council' arid South Northampton shire District Council, registration was refused on the basis that the Registrar was satisfied that the applicants were likely to contravene the fourth data protection principle.

Appeals against these decisions were brought before the Data Protection Tribuna 1. The appeal of the Officer of Rhondda Borough Council was heard separately, the other appeals being disposed of at a combined hearing.

5.6 Rhondda Borough Council

Under the terms of the UK Local Government Finance Act 1988, charging authorities were required to compile and maintain a Community Charge Register. It was specifically provided that the register should include details of the name and address of every person liable to pay the Community Charge. Reasonable steps were to be taken to secure the necessary information. In particular, members of the public were required to complete forms giving details of all persons resident in their household.

The Community Charge was payable by everyone over the age of 18 years. To this extent, a note of the date of birth of individuals who were about to reach their l8th birthday would be required in order for the Registration Officers o fulfil their duty of maintaining the register. In many cases, local authorities, including Rhondda Borough Council, requested the date of birth of every member of the household, regardless of whether they were over 18 or not. Dates of birth are clearly items of personal data.

The appellant applied for registration under the Data Protection Act. This application was rejected by the Registrar, who expressed the view that the inclusion of information relating to date of birth would, subject to very limited exceptions, be irrelevant to the determination whether individuals were liable for payment of the Community Charge. In total eight notices -of refusal and five enforcement notice were served on authorities which proposed to hold information relating to date of birth. All authorities other than the appellant undertook not to include this information.

The appellant argued that many inhabitants of the Rumdda shared surnames and Christian names. The addition of a note of date of birth would limit the possibility that an individual might escape inclusion on the register because his or her identity was confused with some other person of the same name. It was also argued that the inclusion of the information would assist the Registration Officer in the efficient performance of his or her duties.

These arguments were not accepted by the Tribunal. It heard evidence that nationally fewer than one per cent of household contained persons who shared the same surname and Christian name. Although it accepted that the figure night be higher in the Rhondda it did not consider that this justified the appellant's actions. The Tribunal concluded:

> We find that the information the appellant wishes to hold on database concerning individuals exceeds substantially the minimum amount of information which is required in order for him to fulfill the purpose for which he has sought registration ... to fulfill his duty to compile and maintain the Community Charges Register.

The next question to be considered was whether the Registrar had been justified in refusing the application for registration. It was argued on behalf of the appellant that the inclusion of personal data in the form of information about date of birth would not be likely to harm the data subject so long as it ,as used only for the purpose of compiling the Community Charge Register. Given the fact that the Community Charge Register was to be a public document it might be considered unlikely that the information could not be put to other uses, for example by direct marketers. The Tribunal considered that the prime task ,as to ensure the observance of the principle that information held should not be excessive. This was of special importance where the information was sought by a data user who was empowered to require the supply of information by data subjects. The appeal was dismissed and the Registrar's refusal of the application upheld.

5.7 Exceptions to the fair obtaining requirements

A significant exception to the operation of the first principle applies where data is acquired for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty. In such cases, the Registrar may not take any action against the data user involved alleging a breach of the principle where its application would be likely to prejudice the activity in question.

The rationale behind the exception lies in the recognition that law enforcement agencies might reasonably acquire information in ways which might normally be regarded as unfair, for example as the result of overhearing or even eavesdropping on a conversation. It might, however, be considered unfortunate that the Registrar should not be given power to define the concept of fairness in the light of the particular situation of the user involved rather than by providing a near complete exception from the requirement to act fairly. It may also be

noted that the restriction upon the Registrar's ability to act exists even where the data has been acquired unlawfully, although here it may be difficult to sustain the argument that observance of the law would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty.

5.8 Data Protection and the Media

The relationship between media activities and the principles of data protection has proved a somewhat uneasy one. The media, have a n insatiable appetite for data. Investigative journalism in particular relies upon the journalist being able to obtain data;. In some circumstances subterfuge may be involved in the act of obtaining the data and the question will arise how this relates to the application of the first data protection principle and its strictures regarding fair obtaining. It will often be essential to the production of a journalistic that the subject of an investigation should not be aware of the fact.

Comparison might be made with the activities of the police which are subject to specific exclusion from the operation of the first data protection principle. The fact that media activities have not given rise to action under the Act might suggest that the Registrar possesses sufficient discretion in the interpretation of the concept of fairness to make such a blanket exclusion. Some countries, such as the Netherlands and Sweden, provided a total exemption from data protection laws, others provided partial exemption, in the case of Germany, f or example, requiring only that media users comply with requirements relating to data security. Other regimes, including that of the United Kingdom, provided no form of special treatment.

The study identified a potential conflict between the provisions of the European Convention on Human Rights relating to freedom of expression and the right to seek out and impart information and those concerned with the right to privacy. Providing solutions is a difficult task and the Council of Europe contented itself with a recommendation that the potential conflict should be born e in mind in, framing legislation.

A range of media related provisions can be identified in the EU Member States regarding the treatment of the data ranging from providing near total exemption from the requirements of data protection laws to as in the case of the United Kingdom, subjecting them to the full application of the legislation. The Directive's approach can be seen as something of a compromise with Article 9, which is entitled 'Processing of personal data and freedom of expression', providing that:

> Member States shall provide for exemptions or derogation ... for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with tile rules governing freedom of expression.

This is an exceptionally nebulous provision but it must be seen as empowering rather than requiring the provision of specific media related exemptions. The Preamble is somewhat more detailed making reference to the provision of alternative measures such as the submission of reports to the supervisory. agency, to ensure that data subject's rights are not abused. The Registrar, however, has indicated general satisfaction with the present operation of this element of the legislation and it does not appear that significant changes will be introduced.

Storage of Data

The second data protection principle requires that data be held only for one or more specified and lawful purposes. The question whether data is held for a lawful purpose might be determined only retrospectively Holding a list of names and addresses might normally be a non-controversial matter, but if the holder is a burglar and the addresses are of houses which are to be burgled, matters will appear in a different light. For the vast majority of users, the requirement that data be held for a specified purpose is of much greater significance. This is to be determined by reference to the user's entry on the Register. If the purpose is not specified therein, there will be a breach of the second principle.

Both Act and Directive contain provisions relating to the periods of time during which data may be retained. The fifth data protection principle requires that personal data 'shall be accurate and, where necessary, kept up to date, also that data 'shall not be kept for longer than is necessary for that purpose or those purposes'. The Directive contains similar provisions relating to the currency of data but adopts a slightly different formulation relating to retention providing that data is to be:

> . . kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which they data were collected or for which they are further processed.

This formulation appears to allow greater discretion to the data controller than is presently the case-under the Data Protection Act. Given the increasing processing capabilities of computers it may be difficult to determine what steps will require to be take in order to secure the anonymity of particular data subjects.

Processing of Data

Both Act and Directive require that personal data must be processed `fairly and lawfully'. In the Act, the first data protection principle refers to the activities of obtaining and processing. The interpretative paragraph applying to the first principle refers only to the act of obtaining data and the Data protection Tribunal has ruled that a distinction has to be drawn between the two acts and that different factors may be applied in determining whether conduct is fair.'

With the exclusion of the interpretative provisions, there is no further statutory guidance as to the scope of the principle but a series of linked decisions of the Data protection Tribunal relating to the operation of credit reference agencies is of considerable significance.

In determining whether processing is lawful, the major requirement in the Act is that the user should have registered details of the purpose for which the processing is to b conducted. Registration of a purpose will be presumed to give notice to data subjects. The Directive identifies six criteria which will make processing lawful. These require that:

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into such a contract; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the d subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the control or in a third party to whom the data are disclosed; or

The Directive defines the concept of subject consent as 'any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to

personal data relating. to him being processed'. There is no indication in the Directive how the addition of the word 'unambiguously' strengthens this requirement. In other areas, the Directive uses the, again undefined, concept of 'explicit consent'.

It seems clear that both requirements must be more extensive than the general requirement of consent, but it is less so what will be required and what will be the distinction between explicit and unambiguous consent. On the basis of dictionary definitions it might be suggested that explicit consent requires a positive act on the part of the data subject, ie an 'opt in' system, whereas the term unambiguous might not be incompatible with an 'opt-out' system assuming sufficiently clear notice was given to the data subject.

The concept of subject consent has been a feature of the German system since a 1984 decision of the Constitutional Court established the doctrine of 'informational self-determination'. The background to the case lay in the enactment of the Census Act of 1983 which provided for the conduct of a national census and prescribed numerous items of data which were to be supplied by citizens. These included sources of income, educational background, employment, housing, marital status and religious affiliation. It was provided that anonymised census data could be compared with existing registration registries and could also be transmitted to other public authorities acting in the course of their legitimate functions. Holding the relevant statutory provisions unconstitutional, the Court expressed concern that modern data processing techniques would make it a comparatively simple task for apparently anonymous data to be attributed to specific persons.

Although the administration had a legitimate interest in the collection of data of the kinds identified in the Census Act clearly defined conditions of processing need to be required ensuring that under the conditions of automatic collection and processing of personal data the individual is not reduced to a mere object of information. Although the concept of subject consent appears as the first item on the Directive's list, the Home Office have pointed out that it is only one out of six criteria and have suggested that the remaining criteria 'are likely to cover a very high proportion of processing applications'. In many instances processing will be carried out under the terms of a contract with the data subject. An obvious danger in such a situation is that the terms of the contract may be based against the subject's interests.

Direct Marketing

It is a little known fact that those persons who purchase black ash furniture are 20 times more likely to respond to a fashion promotion than those whose tastes are less exotic. Such nuggets of information may constitute interesting trivia to most people, but to those engaged in the retail industry they can represent the path to fortune. Direct marketing is one of the fastest-growing sectors of the economy.

Although it tends to be referred to under the epithet 'junk mail', each item delivered represents a not inconsiderable investment on the part of the sender. In many instances retailers will possess information linking an individual to a purchase and may use this in order to attempt to stimulate further sales. The purchaser of a motor vehicle, for example, is likely to receive a communication from the seller around the anniversary of the purchase in the hope that the buyer might be considering buying a new model. The increasing use of store-based credit cards coupled with the utilization of laser scanning cash points provides retailers with detailed information about their customers and their purchases. There are few technical barriers in the way of processing data so as to be able to ‘talk to every customer in his or her own life style terms' .

It has even been suggested that 'intelligent shopping trolleys' might guide customers towards promotions which analysis of their previous purchases suggests might prove alluring: Assuming that the data users involved have registered the fact that they intend to process personal data for sales and marketing purposes, the only legal barrier to such techniques might come from a determination that such processing is unfair. The use of personal data for purposes of direct marketing has been the cause of some recent controversy.

Reference has previously been made to the Innovations case and data protection implications of list broking. Additionally, however, organizations are seeking to exploit their customer databases by entering into agreements to provide mailings on behalf of other companies. This may take a variety of forms. Analysis of, for example, purchases made with a credit card may indicate that an individual frequently stays in hotels.

The credit card company may then enter into an agreement with a hotel chain to include a promotional leaflet with its statement of account. In this example, no personal data will be transferred between the companies. In a Guidance Note relating to Direct Marketing,' the Registrar has indicated that in certain circumstances use of financial data for such purposes might constitute a breach of confidence.

More recently, action has been taken against a number of utilities engaging in the practice of cross-selling with enforcement notices being served against a number of utilities which sent offers of other products and services to their customers. Significantly, the fact that the utilities offered customers the opportunity to 'opt out' of these offers was not considered sufficient, the Registrar arguing that an 'opt in' system should apply. Treatment of data obtained and used for the purposes of direct marketing constituted one of the most controversial aspects of the Directive. As originally drafted, the legislation would have imposed strict obligations on data controllers to inform subjects whenever data was to be used for such a purpose.

The proposals were weakened in subsequent drafts and as enacted, the Directive offers Member States a choice of control regimes. It may be provided that data subjects be given the right to object to a controller's intention to process or to disclose data for the purposes of direct marketing. No fees are to be charged W this event. It is arguable that this reflects current United Kingdom practice,, especially after the decisions of the Data Protection Tribunal in the Innovations and lingua phone cases. As an alternative, the Directive provides that controllers might be required to give specific notice to data subjects before data is used by or on behalf of third parties for direct marketing purposes.

5.9 Fair Processing

The issues described above establish conditions under which data processing will be considered lawful. As with the requirements relating to the obtaining of data, it is also necessary that processing be carried out fairly. In part this requirement may be satisfied by giving notice to the subject of the purposes for which data is sought but the element of fairness will also relate to the manner in which processing takes place. This is well illustrated by a series of decisions of the Data Protection Tribunal in determining appeals by four major credit reference agencies against enforcement notices served by the Registrar alleging unfair processing.

Credit reference agencies constitute one of the highest-profile sectors of data processors in the private sector. Study of the Registrar's annual reports reveals that a high proportion of complaints from data subjects concern the activities of these organizations. The operation of credit reference agencies has been subject to legal controls since the passage of the Consumer

Credit Act in 1974. The operator of such an agency will require to be licensed as an ancillary credit business. Such licenses will be issued to applicants who can satisfy the Director General of Fair Trading that they are fit and proper persons to action such a capacity. The Act requires credit reference agencies to supply a copy of any information held concerning an individual upon receipt of a written request from that person.

A fee of £1 may be required by the agency. Provision is also made for the correction of any inaccurate information and for details of the change to be transmitted to any third party who had received the inaccurate information within the six-month period preceding the amendment. In two important respects, these provisions are more favorable to the consumer than those applying under the Data Protection Act.

The maximum fee chargeable is only 10% of that provided for under the data protection legislation, while this statute makes no provision for the transmission of information to third parties regarding the correction of inaccurate information. The information held by credit reference agencies will almost inevitably be classed as personal data under the terms of the Data Protection Act.

In the event that processing is conducted using automated equipment, the credit reference agency will have to apply for registration and will be required to comply with the data protection principles. This dual control regime offers advantages at data subjects. They will be able to secure access to data held by credit reference agencies paying the lower Consumer Credit Act access fee whilst the operations of the agency will be subject to the more extensive controls of the Data Protection Act.

The compatibility at certain aspects of the operations of credit reference agencies has been at issue in a number of cases brought before the Tribunal. Several hundred undertakings have been granted licenses under the Consumer Credit Act. Four agencies dominate the United Kingdom market; CCN, Credit and Data Marketing Services, Equifax and Infolink, each of which was the recipient of an enforcement notice served by the Registrar.

5.10 Credit Scoring

The information held by the credit reference agencies and extracted in connection with a particular application for credit might be used in a variety of ways. The established method of operation would be for the agency to supply the information generated to its client, the

potential creditor, leaving the determination whether to extend credit facilities entirely to the recipient. All of the credit reference agencies involved in the Tribunal actions operated on this basis. In a number of cases, the agencies also offered more extensive facilities. Instead of supplying a client with raw data, the client's own acceptance criteria might be applied. These might operate at a fairly simple level so as, for example, to reject all applicants who were not home owners. If searches revealed this fact, a recommendation that the application be rejected would be transmitted to the client. The critical point concerning the agencies' operations , and the aspect to which exception was taken by the Registrar, is that-in all cases searches are conducted by reference to an address rather than a name. Names, apparently, constitute an inefficient means of identification.

A glance at any telephone directory will show that most surnames appear more than once. Even full names are unlikely to be unique and most recipients of 'junk mail' will be aware of the many and various permutations of names and initials that may appear on envelopes. By contrast, address-based information is easy to obtain and to verify.

The consequence of such a practice might be that a search resulting from an application for credit by one individual would retrieve information about previous residents at the address given and as to members of family or others who shared the address with the applicant. The use to which this information might be put would vary from agency to agency and from creditor to creditor. It was accepted, however, that individuals might be denied credit because of the extracting of detrimental information relating to third parties, and that this might cattle them distress.

The extraction of third party data in making decisions about an individual applicant was considered by the Registrar to constitute unfair processing of personal data and, as such, contravened the first data protection principle. After discussions with the credit industry failed to provide an acceptable solution, enforcement notices were served on the four major agencies in August 1990. The terms of these notices were virtually identical, requiring the recipients to ensure that:

> . . . from the 31st day of July, 1991 personal data relating to the financial status of individuals ceases to be processed by reference to the current or previous address or addresses of the subject of the search whereby there is extracted in addition to information about the subject of the search any

information about any other individual who has been recorded a s residing at any time at the same or similar current or previous address as the subject of the search. A considerable number of issues were raised in separate Tribunal proceedings hearing appeals by each agency. Given the identical factual backgrounds it may be more convenient to consider the cases by reference to the issues involved.

This definition encompasses a considerable range of operations. In the case of credit reference agencies it was the act of extraction that was critical to the decisions. Relating the definition to the first data protection principle, the question to be answered by the Tribunal was whether the extraction of data by the credit reference agencies was to be considered unfair. An initial argument put forward on behalf of CCN sought to draw a distinction between the extraction and the use of the personal data.

The extraction of information, typically by causing the information to be displayed on a monitor was, it was argued, a 'value-free operation and not susceptible of judgement by reference to criteria of fairness. What the Registrar was objecting to, it was argued, was the use to which the data was subsequently put-perhaps to refuse an application for credit. Nowhere in the first data protection principle is there any reference to the use to which personal data might be put, mention being made only of the acts of obtaining and processing data. This line of argument was rejected by the Tribunal. Such an approach, it was held, would rob the first data protection principle of almost all meaning.

Reference was made to the long title of the Data Protection Act which described it as an `Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of the use of such information'. This made it clear that it sought to control not the technology but its human controllers. Although the data supplied by CCN's computers would be used subsequent to the actual processing, the computers could operate only in accordance with their programs. These specified the criteria by which information was to be extracted. The extraction was not, therefore 'value-free' and the activity had to be judged by reference to the statutory criteria of fairness. The second element of Equifax's appeal concerned the requirement that processing be conducted by reference to the data subject.

Equifax, it was argued, in common with the other agencies, extracted information by reference to address rather than name. This argument was rejected by the Tribunal. Account,

it was held, had to be taken of the intended purpose of the processing. If this was to obtain information concerning a living, identifiable individual, the Act would apply. It was noted that one of Equifax's registered purposes is to provide 'information relating to the financial status of individuals'.

The company was well aware that its customers sought the information in connection with their transactions With individuals and that the results of its processing would affect . these persons. Again, such a conclusion is to be welcomed as an indication that the Tribunal will 'lift the veil' in the event that processing is carried out by reference to any attribute other than name.

Applying these criteria, the Tribunal considered evidence submitted on behalf of the appellant arguing that the unavailability of third party information would render their operations less effective. The consequence would be either an increase in bad debts or the denial of credit to persons who might otherwise have been accepted. It might even be that certain creditors would cease to operate in the consumer field.

The Tribunal accepted that the operation of credit reference agencies provided benefits. It noted that the Act essayed no definition of the word 'fairly' but held that the prime purpose of the legislation was to protect the rights of the individual. Whilst the interests of the credit industry should not be ignored, primacy must be given to the, interests of the individual applicant. On this basis it was considered

> . . . unfair for a credit reference agency, requested by its customers to supply information by reference-to a named individual, so to program the extraction of information as to search for information about all persons associated with a given address or addresses notwithstanding that they may have no links with the individual the subject of the inquiry or may have no financial relationship with that individual.

A further argument concerning the status of extraction as a form of processing was also argued before the Tribunal. Extraction as an automatic process, it was argued, was normally value-free and could be considered objectionable only if it involved a breach of the applicant's right to privacy. The extraction of third party information could not produce this effect.

Given the absence of any general right to privacy within the UK, such a restricted interpretation would render the first principle of very limited value. The Tribunal rejected

such x1 interpretation, holding that privacy-related Matters constituted only one form of potentially unfair extraction and reiterated the view expressed in CCN that objection could be taken to the extraction of irrelevant third party information.

It was also argued that much of the information field in and extracted from county courts, was from Infolink's computers, for, example judgments such data should be readily available. Whilst not disputing this argument, the Tribunal pointed out that they were concerned with a much narrower issue: whether the extraction of this information in connection with a search relating to an unconnected individual cold be considered fair. The answer to this must be in the negative.

A similar response was given to the suggestion that the agencies' customers could have discovered the same information for themselves. This was considered to be an unlikely possibility and again the point was made that one of the purposes of the Data Protection Act was to control the capability of computers to bring information together from a number of disparate sources and provide the possibility of extracting elements which might or might not be relevant to a decision in hand.

Another basis for appeal concerned the applicability of exceptions concerned with data held for the purpose of the prevention or detection of crime. Not only was such data partially excluded from the operation of the subject access and the non-disclosure principles but it was provided that in determining whether to take any form of action against a data user, the Registrar could not invoke the first data protection principle in any case where its operation 'would be likely to' prejudice the purposes specified.

Although the application of this provision to the credit reference field may appear a little obscure, it was argued that one of the major reasons why credit reference agencies sought information about individuals was to minimize the risk of fraudulent credit applications being successful. Anything which produced this effect, it was argued, would fall under the statutory exemption. Evidence was led to show that the operation of the Credit Industry Fraud Avoidance System, access to which might be obtained through Equifax, led to the identification of 7,000 frauds during the year 1990.

The implications of this argument are clearly significant and capable of applying beyond the credit field. In the event, the Tribunal adopted a restrictive view of the application of s 28.

Data would be exempt in any case where the attainment of the specified purposes would otherwise be prejudiced but justification would be required in each individual case. The vast majority of honest applicants could not be deprived of their rights because of the existence of a comparatively small number of fraudulent claims.

The phrase 'would be likely to prejudice' was to be inter related in that sense and not in the sense of 'might , conceivably prejudice'. This element of the Tribunal s decision is significant in that it makes it clear that the criminal exceptions of s 28 may be invoked by data users other than law enforcement agencies. It is also clear, however, that its application will have to be justified in each particular case.

The form of the enforcement notice

In all of the credit reference agency decisions the Tribunal accepted that a breach of the first data protection principle had occurred sufficient to justify the Registrar in serving an enforcement notice. In, all the cases, however, the Tribunal considered that the terms of the notice were excessively broad.

The value of reliable credit reference and credit scoring systems was accepted, the Tribunal commenting that it was:

> very conscious of the benefits of reliable credit reference and credit scoring systems in preventing over-commitment by debtors, a measure very much for their benefit and that of the community, and in ensuring a well-managed credit system for the benefit of potentially sound debtors and of the. credit and supply, industries.

Although the unrestricted use of third party information was considered objectionable, the Tribunal did accept that information relating to members of the applicant's immediate family or to persons with whom the applicant shared property might be relevant to a decision concerning the grant of credit.
To this extent the terms of the Registrar s enforcement notice would be varied to permit the extraction of third party information in a restricted set of circumstances.

> Where the third party is recorded as residing at any address concurrently with the applicant and where the third party shares the same surname and any recorded forenames or initials as the applicant.

An example of this situation might see a parent and sibling sharing the same name and living at the same address. In such a case it might be difficult if not impossible for the credit reference agency to be able to avoid extracting information about the non-applicant. Extraction of third party data will not be considered unfair in this situation except where the agency possesses information from which they should reasonably be aware that there are two parties involved. This might be the case when parents, perhaps acting in response to previous incidents, have informed the agency that they were not willing to accept responsibility for the actions of their child - or vice versa.

> Where the third party is recorded as residing at any address concurrently with the applicant and where the third party has a name sufficiently similar' to that of the applicant to make it reasonable for the agency to believe that the parties are one and the same.

The application of this exception is subject to the same proviso as that described above regarding the existence of information contradicting the presumption of commonality. The application of this exception must be less certain than its predecessor. It would seem reasonable for it to apply in the case of minor variations in initials and perhaps even of spelling of surnames. Any recipient of 'junk mail' will be aware of the many and various formats in which names may be presented.

> Where the third party shares the same or a sufficiently similar surname as the applicant and it is reasonable for the agency to believe that they have been living as a member of the same family as the subject in a single household'.

This exception will allow extraction of information relating to members of the applicant's family. It would appear that this would apply even where the third party is residing, at a different address. Extraction will not be permitted where the agency possesses information which makes it reasonable for it to believe that there is no financial connection between the applicant and the third party where the third party does not share the same surname as the applicant but, from information possessed by the agency prior to extraction, it is reasonable to believe the third party and the applicant are one and the same person.

This exception will apply in the situation where the applicant is suspected of using a variety of names-perhaps in order to obtain credit by means of fraud. It is subject to the same proviso as operates in the previous exception although the scope for its application must be limited.

Where the third party does not share the same surname as the applicant but, from information possessed by the. agency prior to extraction, it is reasonable to believe has been living as a member of the same family in a single household.

This exception will operate in the situation where unmarried persons share the same address but will not apply where the agency possesses information from which they should reasonably conclude that there is no financial connection between the third party and the-applicant.

The scope of these exceptions is potentially broad. An agency will not be able to extract information about third parties previously resident at the same address as that pertaining to an applicant. In cases where there appears to be some link the agency will be able to extract third party data in the absence of specific information. The onus will lie with data subjects to supply any information disclaiming links with other persons and it may be doubted how effectively this might be accomplished in anticipation of the extraction of data. Most likely, information may be supplied only in response to the unfavorable use of the information extracted.

5.11 Caller Identification

Systems of caller identification allow the recipient of a phone call to cause to be displayed the number from which the call originates. Display of the caller's number at the time when the phone rings can, at the least, allow the recipient to decline to answer. More significantly, the facility has been welcomed by people who have had experience of 'nuisance calls'.

From the data protection perspective, the operation of such a system calls for the processing of what will often be personal data in the form of the caller's telephone number. If such displays offer advantages for the recipient, they may prove less desirable for the party making the call. When the call is made to a commercial organization enquiring about goods or services, details of the number may be recorded.

The enquirer may then be in turn the recipient of telephone calls offering to supply goods or services. At a more significant level, a party may be unwilling to make calls to support agencies such as those for alcoholics or drug addicts save under conditions of anonymity. Even calls to the police might be subject to the same reservation.

As with so many aspects of the topic of privacy, a conflict of interests may exist. The recipient's wish to be protected from unwelcome telephone calls may not always be compatible with the caller's wish for anonymity. The proposed EC Directive 'concerning the protection of personal data and privacy in the context of public digital telecommunications networks" proposed that callers should be enabled to eliminate, either permanently or in the context of a particular call, the display of their telephone numbers.

Equally, however, a subscriber should be able to refuse to accept any calls where the caller's identity was not transmitted.' By way of exception to these provisions it was proposed that telecommunications authorities might override the elimination of caller identification where they were acting following a complaint from a subscriber concerning receipt of malicious calls or under the terms of a court order in connection with the prevention or detection of a serious criminal offence. It was further proposed that the override facility must be made available to the emergency services.'

There appears little immediate prospect of the Directive being enacted. The example does illustrate how what might appear initially to be a noncontentious application of technology raises more complex issues. Certainly, it is possible for the Registrar to institute proceedings under the Data Protection Act on the basis that the activity involves the unfair processing of personal data. This does appear somewhat peripheral to the nature of the activity in, question and raises the question of how far an omnibus data protection statute can regulate satisfactorily the vast spectrum of processing activities conducted using the ubiquitous computer.

Although views may differ concerning the nature of the solutions proposed, the EC proposal suggest' that a more sectoral approach building upon general data protection principles may offer an appropriate way forward.

5.12 Processing of Statistical Data

As evidenced by the German census decision, much personal data is obtained and processed for statistical purposes. The German court drew a distinction between statistical and personality-related data. Personality-related data requires that the purpose for which the data is obtained should be determined precisely and the amount of data sought limited to the minimum necessary to achieve the stated purposes. For statistical data, however, a narrow

and concrete purpose limitation cannot be required. It is a characteristic of statistics that after statistical processing they should be utilized for the most variable purposes . . .

The prohibition of dissemination and utilization for statistically processed data would be contrary to purpose'. Much will of course depend upon the nature of the data in question. Where individuals cannot be identified there will be no question of the data protection regime applying. Thus, for example, the processing by a super market of data relating to goods purchased will not be affected so long as no details are included of the individuals making the purchases. As discussed above, the Directive's definition when an individual is to be considered identifiable is considerably broader than that adopted in the Act, referring to identifying information held by the data controller or by any other person.

The Data Protection Act presently provides that where personal data is held and used, the first data protection principle relating to the fair obtaining of data will not be breached by reason only of the fact that the subject was not informed that the data would be used for such purposes.' Again such data may be kept indefinitely and will be exempted from the subject access provisions. The Directive contains similar provisions although it refers to the more qualified purpose of 'scientific research' rather than the Act's 'research'.

The requirements to notify the data subject will not apply where data is obtained from third parties for statistical purposes or for the purposes of historical or scientific research where the provision of information will be impossible or involve an effort disproportionate to the risks involved. Such data will also be exempted from the requirements relating to duration of record keeping.' In all cases, however, the exemption will only apply if national implementing measures provide appropriate safeguards. The Directive refers in particular to the need to 'rule out the use of the data in support of measures or decisions regarding any particular individual'.

5.13 Accuracy and Timorousness of Data

The fifth data protection principle requires that personal data shall be accurate and, where necessary, kept up to date. Data is regarded as being, inaccurate when it is 'incorrect or misleading as to any matter of fact'. In the event that personal data is inaccurate, a data subject may be entitled to seek its rectification' and to be compensated for any damage or

distress suffered by reason of the inaccuracy.' The question whether data is accurate will not always be susceptible of a straightforward answer.

Expressions of opinion may not be compatible with objective verification. Even with factual data, difficulties may arise where this has been received from a third party. A statement may be in the format: 'Fred Smith informs us that Joe Bloggs has defaulted on three loan agreements.' If it is assumed that Joe Bloggs is in reality a person of the utmost financial probity, can it be said that the statement is false? The view was expressed in Parliament that such a statement would be an accurate record 5f the information supplied. In the situation where a data subject is seeking compensation on the ground of the inaccuracy of data, a defense is provided to the user where the data has been supplied by a third party.

In order to benefit from this defense, he data must be marked as having been so received and, in the event that its accuracy has previously been challenged by the subject, an indication to this effect must be linked to the data in such a way that the two are always presented together. Although the Act is silent on the point, it would appear reasonable that similar steps should be required in order to demonstrate conformity with i.e., fifth data protection principle.

The second element of this principle requires that necessary updating of information shall be carried out. The question whether updating is required will be dependent upon the nature of the data and the purpose to which it will be put. If the data is merely a record of a transaction between the data user and the data subject no updating would be either necessary or justified. Where the information is being used as the basis for continuing decisions and actions, regular updating may be essential. Thus where information is to be used for assessing an employee's suitability for promotion, an indication of periods of absence would require to be supplemented by any explanations which might subsequently have been provided.

Duration of Record Keeping

Linked to the issue of the topicality of data are the provisions of the sixth principle which require that data should be retained for no longer than is necessary for the attainment of the purpose for which it is held. The Directive contains an equivalent provision. Neither instrument expands on this provision. In many cases data users will be under an obligation to maintain data for a specified period of time, e.g. solicitor-client data.

In more general terms there would appear justification for retaining data until the expiry of any limitation period for possible legal action. Save in the situation where data is maintained as a matter of historical record 2 the sixth data protection principle would appear to require that users operate some form of policy for monitoring their data holdings and removing items which are no longer of value or relevance to their activities.

5.14 Data Security

Under the terms of the final data protection principle data users and the operators of computer bureau are obliged to ensure that 'appropriate security measures' are taken to guard against the risks of unauthorized access, alteration, destruction, disclosure or loss of personal data. This principle requires appropriate rather than absolute security measures. In determining the level of the security required, the Act indicates that account should be taken of the nature of the data and of the harm that might result from a breach of security

The comparable requirement in the Directive is that, taking account of the state of the art and making an assessment of costs and risks involved:

> ... the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network...

The Registrar has identified a considerable number of matters which are relevant to data security Account might be taken of the physical security of premises, of any security measures incorporated into computer systems, for example password requirements, of the level of training and supervision of employees. A number of instances have been reported of the purchasers of second-hand computers discovering that data belonging to the original owner remained in the machine's memory

Such lapses might constitute a breach of the principle, as might any deficiency in respect of the disposal of print outs of computer-generated data. In 1992, the European Communities adopted a 'Decision in the field of the security of information systems'. This is concerned essentially to establish the basis for Community action and calls, inter alia, for the development of specifications, standardization, evaluation and certification in respect of the security of information systems such measures might be of significant value in the field of

data protection, although the diversity of processing activities might defeat any simple form of classification.

At least in the case of personal data, it makes it clear that a duty to maintain security is imposed upon the data user. In some senses, the user might be regarded as a custodian requited to safeguard the data subject's interests. It is now a matter of historical curiosity that until the passage of the Computer Misuse Act in 1990 a data user whose computer system was penetrated by computer hackers might face possible criminal prosecution. Admittedly, the risk of this is extremely remote, requiring that the user willfully or recklessly fail to comply with the terms of an enforcement notice served by the Registrar,' but until the entry into force of the 1990 Act, the hacker would not have committed any offence.

Use of Data

In examining the controls relating to the use to which personal data may be put, attention must be concentrated upon the third data protection principle. The interpretative provision relating to this principle makes reference to the user's entry on the Data Protection Register. If the disclosure is to a person or category of person specified therein, there can be no question of breach of the principle. Normally, any further disclosures will constitute a breach of the principles. The Act's provisions, however, serve to sanction a variety of unregistered disclosures.

Exceptions to the Non-disclosure Principle

Few data users might anticipate a need to make disclosures to law enforcement agencies at the time of completing their Register entry. Circumstances might arise, however, in which they, and possibly also the data subject, might wish that information should be disclosed.

An example might concern the situation where details of a person's attendance at work might be relevant in a criminal investigation. To avoid the situation where a user could not legally assist criminal investigations, the Act provides that the non-disclosure principle will not apply where data is disclosed by a user in the reasonable belief that this is for purposes connected with: .

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; and
- the collection or assessment of any tax or duty.

Subject to the condition that a failure so to disclose would prejudice the attainment of the purpose in question. Disclosures may also be made by any data user where this is for the purpose of safeguarding national security. The need for some exception in this area is not seriously questioned. None the less, Sir Norman Lindop has criticized this provision as 'perpetrating a fraud on the public'. The basis for this opinion is that a cardinal feature of the legislation lies in its promise to the public that the purposes for which their data may be used will be a matter of public record yet, in these significant areas, the Act sanctions contrary and secretive disclosures. The criticisms which may be made of this exception are germane to many aspects of the legislation.

The need for some provision is unarguable but rather than attempting to analyze the extent of the requirements and make limited provision the Act provides a blanket exception. There is no requirement that the disclosure be in connection with a serious offence, there are no provisions regarding the procedure to be followed. Although both parties may face internal disciplinary measures, there is nothing in the Data Protection Act to prevent a request for disclosure being made by the most junior police officer and acceded to by the most junior member of the data users staff. No records need be kept of the disclosure and no form of notification given to the Registrar.

5.15 Legal Requirements or Advice

Where disclosure is required by any other statute, by the order of a court or where it is made for the purpose of obtaining legal advice or in the course of legal proceedings the non-disclosure principle will not apply.

5.16 Disclosure to the data subject etc.

Disclosure may always be made to the data subject or to a person acting on his or her behalf Disclosure may also be made in any circumstances where the subject has consented to this taking place. These provisions appear, and in many instances will be, quite innocuous. It may be noted initially that the provision empowers rather than requires disclosure. In cases where

the data subject requests disclosure there may be an overlap with the subject access provisions described in the following chapter.

In instances where the disclosure is made to some third party, it may be uncertain whether the data subject's consent is genuine. The issues may be more relevantly discussed in the context of subject access, but there appears a danger that extending the individual's control over personal data might weaken his or her position in certain respects.

5.17 Preventing Injury

A final exception to the non-disclosure principle applies where the data user reasonably believes that disclosure is urgently required for preventing injury or harm to the health of the data user or Eo any other person. It is difficult to identify situations in which this provision may be invoked. In cases where the data is medical in nature it may be that the possibility of disclosure would have been anticipated at the time of registration.

A possible scenario might see details of an individual's holiday address held on a travel agent's computer. If information came to light that prior to departure the person involved had been exposed to a dangerous virus and should receive urgent medical attention, disclosure of the data by the travel agent might be justified under this provision.

5.18 The Exceptions in Perspective

Although criticism has been made of a number of the provisions restricting or exempting the application of the data protection principles, it is important to bear in mind that these are exceptions and, more significantly, that prior to the introduction of the Data Protection Act few legal controls operated concerning the use to which personal data could be put. To this extent, the Act undoubtedly improves the lot of the individual and the only valid cause of criticism is that it eschews the opportunity to confer more significant benefits. In the case of the exemptions relating to crime and taxation, the subject matter will remove them from the application of the Directive.

The principles behind the remaining exemptions would appear to be in conformity with the Directive's requirements. Where the Act, and present proposals for reform, might be

criticized is not for making provision for exemptions in the areas specified, but in the absence of procedural or monitoring requirements to provide a check against misuse of the exemption. One safeguard might be to require that users notify the Registrar of instances where disclosures have been made in reliance upon one of the exemptions.

5.19 Data Matching

The practice referred to as data matching has attained considerable publicity. Operating principally in the public sector, it can be seen as an equivalent to some of the direct marketing techniques described above but with the essential difference that it involves searches across a range of data bases controlled by different Government departments. In the past strict controls have limited or in many cases prevented the exchange of data held by different departments but provisions in the Social Security (Administration) Fraud Act 1997 provide a statutory basis for the exchange of information between the Department of Social Security and a range of other departments including the Inland Revenue for the purpose of detecting fraud.

Information may also be exchanged with local authorities responsible for the administration of various housing and council tax benefits with the view to identifying inconsistencies. With the development of computer networks, it is a comparatively simple matter for such exchanges to take place automatically so that although there may not be a single massive computer data base, the effect may be chillingly similar. Although the application of data matching is a new phenomenon for the United Kingdom, the technique has been applied in a number of other countries including Australia, New Zealand and the United States.

In New Zealand the practice has been attacked by the Privacy Commissioner who has challenged both the ethics of placing innocent individuals under surveillance as well as the benefits obtained by government. Many calculations, it was suggested, were 'based on frankly heroic assumptions' . Further support for skepticism comes from the United States where a General Accounting Office report on the practice:

> . . . found many problems with implementation of (statutory provisions regulating data matching) including poor quality or non-existent analyses. In 41 per cent of cases, no attempt was made to estimate costs or benefits or both. In 59 per cent of cases where costs and benefits were estimated, the GAO found that not all reasonable costs and benefits were considered . . .

Indications of the scale which data matching activities can assume come from Australia where a programme similar to that introduced under the 1997 Act anticipates between 375-750 trillion attempted file matches each year. Vast to human eyes, these figures are eminently manageable using computer technology.

The Australian figures illustrate a further consequence of the activity. Almost no-one can escape being the subject of data matching. Every data base contains errors and the inevitable consequence is that suspicion of wrongdoing may fall upon innocent individuals. Data matching can, of course be put to positive as well as negative uses. In Parliament during the passage of the 1997 Act the suggestion was made that data matching techniques could be used to identify individuals who were entitled to benefit but had not submitted a claim.

In terms of data protection, the exemptions from the non-disclosure principles are sufficiently broad to justify most of the disclosures of data which would occur in the context of data matching. Following the expression of concerns by the Data Protection Registrar at the privacy implications of the new provisions, the Government agreed to enter into discussions with a view to compiling a code of practice and offered an undertaking that data matching would not commence until this work had been completed.

5.20 Codes of Practice

One of the most notable features of the data protection principles is their generality. Given the range of applications across which they have to be applied and the multitude of users subjected to regulation, it is difficult to envisage any other approach. In its report, the Lindop Committee advocated that statements of general, principle should be supplemented by around 50 statutory codes of practice. As originally introduced, the Data Protection Bill contained no reference to codes of practice. At a late stage in its Parliamentary passage an amendment was accepted which imposes a duty upon the Registrar:

> where he considers it appropriate to do so, to encourage trade associations or other bodies representing data users to prepare and to disseminate to their members, codes of practice for guidance in complying with the data protection principles.

In common with many of the duties imposed upon the Registrar, this requirement is formulated in such a manner as to afford considerable discretion to the Registrar. In the years subsequent to the passage of the Act a considerable number of codes have been produced giving guidance as to the interpretation of the principles within specific areas of activity.

In law, such codes possess only evidentiary value. Many of the codes contain a statement from the Registrar to the effect that:

> Observance of this code does not constitute an assurance that I will accept in all cases and without qualification that data users have complied with the Act. However, in considering relevant complaints it is my intention to give careful regard to whether the data user concerned has been complying with his code of practice and will take such compliance as a positive factor in his favour.

Not all the codes have received the Registrar's unqualified blessing. That produced by the Committee of Vice-Chancellors and Principals contained advice as to a method by which students might legally be prevented from obtaining access to their examination marks. This prompted the comment that:

> I note the comments made . . . about examination marks. Whilst the procedure envisaged in this section is not wrong in law, it is likely to give rise to difficulties and I find it disappointing that it should appear in an otherwise positive document.

The issue of the status of codes of practice was discussed in the Tribunal decision of Innovations v Data Protection Registrar. The substantive issues concerned with the question whether the appellant's information gathering practices conformed with the requirement of the first data protection principle that data be obtained fairly has been considered earlier. It was also argued on behalf of the appellant that its practices conformed with a code of practice adopted by a relevant trade association, the Advertising Association.

The strength of this argument was undoubtedly weakened by the fact that in a foreword to the code, the Registrar had intimated that the Association's view of what was necessary to ensure fair obtaining of data 'differs from my own' and also by the fact that the Council of the Advertising Standards Association and another trade association, the Direct Marketing Association had adopted rules requiring prior notification to data subjects as part of their codes of conduct.

5.21 Codes under the Directive

The Directive envisages a substantial role for codes of practice to operate at both a national and a Community level. The Preamble recognizes that:

Member States and the Commission in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the operation of this Directive, taking account of the specific circumstances of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation.

This much merely restates present practice under the Data Protection Act. In implementing the provision; however, Article 27 provides that draft codes are to be submitted to the national supervisory authority which is to ascertain 'whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive'. In making this determination the authority may seek the views of data users or their representatives. This would appear to mark a significant advance on the present situation where although, as cited above, the Registrar may express the view that the terms of a code do not comply with the requirements of the legislation, there is no precedent for a positive assertion that the code does comply. Such a development would also go at least part of the way to meeting the suggestion of the Registrar in his 1989 Review of the working of the legislation that upon receipt of the Registrar's endorsement, the provisions of a code should have a status equivalent to the Highway Code, i.e. that although breach of its provisions would not itself constitute an offence, this could be taken into account in determining whether any provision of the legislation had been violated.

Provision is also made for the establishment of Community codes. These may be referred to a Working party established under the Directive with the remit to examine the conformity of national implementing measures with the Directive's requirements, to advise on the level of data protection applying in third countries, to advise the Commission on any amendments to the Directive and 'to give an opinion on codes at Community level'.

The Working Party may also seek out the views of data subjects or their representatives before determining whether the draft is in accordance with national implementing provisions. In this event, the 'Commission may ensure appropriate publicity for the code'. Given the requirement that the Directive be implemented in all of the Member States it is not clear what will be the role of Community codes.

5.22 Short Summary

- Personal data shall be held only for one or more specified and lawful purposes.

- Inorder to secure the delivery of goods the customer should provide some personal data.
- The community charge was payable by everyone over the age of 18 years.
- The Directive contains similar provisions relating to the currency of data but adopts a slight different.
- Processing is necessary in order to protect the vital interests of the data subject.

5.23 Brain Storm

- Discuss about Acquisition of data.
- Give note on Data Protection and the media.
- Explain fair Processing
- Discuss caller Identification.
- Describe Data Security.

Lecture 6

Data Protection

Objectives

In this Lecture you will be able to

- Know about Transborder Transnational data Flows (TBDFS)
- About Transfer to another convention state.
- Describe Transborder data Flows and the directive.

Coverage Plan

Lecture 6

6.1 Snap Shot

6.2 Transborder Transnational Data Flows (TBDFS)

6.3 National controls over Transborder data flows

6.4 Establishing conformity with the conventions requirements

6.5 Transfer to another convention state

6.6 Transfer to a nonsignatory state

6.7 Transborder data flows and the directive

6.8 Short Summary

6.9 Brain Storm

6.1 Snap Shot

The Data Protection Act applies to all data users who control the contents and use of personal data from within the United Kingdom. The question whether an undertaking can be considered for resident in the United Kingdom is one which arises in a number of contexts and which may produce different results. As the Registrar has commented, a company could be regarded as resident in the United Kingdom for the purpose of the Data Protection Act but not for taxation purposes. In the event that the company is not considered resident, it may be that it will be represented in the United Kingdom by a 'servant or agent' who will be classified as a data user for this purpose.

It may also be the case that the undertaking which carries out the processing may be regarded as a computer bureau for the purpose of the legislation. Similar problems arise when data relating to United Kingdom data subjects is processed abroad. In many instances, the data will remain under the legal control of the United Kingdom based user who will therefore be subject to the legislation.

The view has been taken by the Registrar that jurisdiction will be claimed even where all aspects of the processing are carried out abroad but where it is intended that the data will be used in the United kingdom-regardless of the form in which it is imported. The correctness of this interpretation has not been tested before the courts or the Data Protection Tribunal.

In the Directive it is provided that Member States are to apply national laws where processing 'is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'. Such a formulation may lead to extra-territorial application of national laws.

There is potential for overlapping jurisdiction in the situation where multinational undertakings process personal data in a variety of Member States. In its Consultation Paper, the Home Office asserts that:

> While some of the provisions relating to geographical extent are clear enough, others are obscure and potentially ambiguous. There is, therefore, the potential for inconsistent approaches being adopted in different Member States. The danger is that this could make it possible for the

> national law of more than one Member State to apply to a single processing. operation, or for no Member State's law so to apply.

The multiple jurisdiction situation would appear to be an inevitable consequence of the free movement of data within the Union. Given that a major purpose of the Directive is to harmonize the laws of the Member States, such a result should not be excessively burdensome for data users and indeed corresponds to the United Kingdom Registrar's interpretation of the existing situation under domestic law. It is difficult to envisage that a reasonable interpretation of the Directive's terms could produce a situation where no national law applied.

6.2 Transborder transnational data flows (TBDFs)

Transborder data flows have been a feature of life since the dawn of communication. In more recent times the international postal and telephone systems have expanded greatly the nature scale and operation of such transmissions.

The advent of computer communication expands the scale of transborder data flows still further whilst, as has already been stated, the development of the internet makes national geographical boundaries effectively redundant.

Although technical developments challenge increasingly the effectiveness of national regulation there is a long history of states attempting to control international data transfers. The International Telecommunication Union was founded (as the International Telegraph Union) in 1865 to try to avoid the situation where concerns at the implications of international transfers on national security resulted in such telegrams being:

> . . . sent to the terminal at the border, decoded and walked across to the next country where the message was again encoded and sent on to the terminal at the next border and so on.

In keeping with a tradition of history's tendency to repeat itself, concerns at the implications of transborder data flows have been evolved paralleling the development of national data protection statutes. Typically the fear is expressed that an absence of control may result in evasion of national controls. As has been stated:

> . . . protective provisions will be undermined if there are no restrictions on the removal of data to other jurisdictions for processing or storage. Just as money tends to gravitate towards tax havens, so sensitive personal data will be transferred to countries with the most lax, or no data protection standards. There is thus a possibility that some jurisdictions will become 'data havens' or 'data sanctuaries' for the processing or 'data vaults' for the storage of sensitive information.

Without exception all national provisions controlling transborder data flows have been linked to data protection statutes with controls justified on the basis of safeguarding the position of individuals. It may be noted, however, that personal data is involved in only between 2% and 5% of transborder data flows, with the bulk of data traffic concerning commercial and financial data. Such a situation has prompted comment to the effect that:

> When governments and international bodies regulate TBDFs, it is often stated that it is done for the protection of personal privacy, national security or national sovereignty. Seldom will it be admitted that the rationale behind regulation is national economic welfare. Often those subjected to regulation accuse regulators of using privacy, security or sovereignty to hide protectionist measures. They are often correct in making such assumptions.

A major problem facing regulators is that it is impossible, without engaging in total monitoring of all data flows, in itself an undesirable practice, to distinguish between various forms of data flow. Numerous reports have identified the potential for conflict between the general desirability of the free flow of data, essential for the world-wide provision of services such as credit cards and the threats to individual privacy inherent in such transfers. One such report stated:

> . . . the question of transborder data flows will undoubtedly become increasingly important in the future and the question will increasingly arise as to which should take priority; the need for efficient economic information or the need to protect individual privacy.

The Council of Europe, in considering the importance of privacy implications of new technology, referred to the multifarious means of international communication made now available through network, satellite communications, concluded that:

> . . . as the volume of transborder flow increases, the control possibilities diminish. It becomes much more difficult, for example, to identify the countries through which data will transit before reaching the authorized recipient. Problems of data security and confidentiality are heightened when data are piped through communication lines which traverse countries where little or no attention is accorded to issues of data protection . . .

In brief, when advanced communication networks enable businessmen on foreign travels to access their enterprises' data bases via hand-held computers plugged into sockets available in airports and to down-load data instantaneously into their computers across vast distances, the issue of national regulation of transborder data flows becomes problematic indeed.

Clearly these issues can be resolved only through a much wider degree of international agreement than has occurred to date. The issues of regulation span almost every aspect of political, economic and legal activity Particularly in the third world, transborder data flows have been regarded as ushering in a new era of economic colonialism'. Even in the first world, concern has been expressed at the scale of the United States' dominance in the field. The provision of a satisfactory legal regime must be regarded as one of the major challenges facing international organizations today.

6.3 National controls over Transborder data flows

The approach which has generally been adopted by states implementing data protection statutes has been to impose some form of control over the transfer of personal data unless there can be a degree of assurance that data protection standards will be observed in the recipient country.

The extent of national controls varies. In Sweden and Austria, transborder data flows out with those countries which are signatory to the Council of Europe Convention require to be licensed by the data protection authorities. In other countries such as the United Kingdom, data users will be required to register their intent to make such transfers which may then be carried out unless specifically prohibited. As has been described, the United Kingdom experience is that this is an unlikely prospect.

Although the Data Protection Act. provides that the Registrar may serve a transfer prohibition notice. Where he is satisfied that 'the transfer is likely to contravene or lead to a contravention of any of the data protection principles', to date, only one such notice has been served by the Registrar. This prohibited the transfer of personal data in the form of names and addresses to a variety of United States organizations bearing such titles as the Astrology Society of America, Lourdes Water Cross Incorporated and Win with Palmer Incorporated.

These companies which had been involved in the promotion of horoscopes, religious trinkets and other products in the United Kingdom, were the subject of investigations by the United States postal authorities alleging wire fraud and a variety of other unsavory trading practices. At the international level, the Council of Europe Convention and the OECD Guidelines have sought to promote the free movement of data, at least between those states maintaining common standards of data protection.

6.4 Establishing conformity with the convention's requirements

Assuming that a data transfer which may involve personal data is being considered by an undertaking located in a state signatory to the Convention, the question arises how conformity with the Convention's requirements may be assured? In the situation where the transfer is to be made to another signatory state, few problems will arise. As stated previously, one of the purposes of the Convention is to safeguard the free flow of data between its signatories. More difficult issues arise where the transfer is intended to be made to a state which has not signed the Convention. Although the Convention makes provision for signature by states which are not members of the Council of Europe, to date this has not occurred and the Convention applies to a small proportion, at least in geographic terms, of the globe.

6.5 Transfer to another convention state

As with all good principles, similarly free movement of data between signatory states is subject to a number of exceptions. Reference must first be made to the fact that the Convention prohibits restrictions to data flows only where these involve personal data and where this is 'for the sole purpose of the protection of privacy'.

Restrictions may be justified on other grounds such as the protection of economic interests. It is to be noted that, unlike the European Convention on Human Rights, the data protection instrument contains no provision for the establishment of dispute resolution machinery. In the event that a signatory state places restrictions on data transfers no legal mechanism exists

whereby the conformity of this to the Convention may be established. Restrictions upon data flows may be justified in two further situations.

Where a signatory state has taken advantage of one or more of the exceptions provided in the Convention, for example in restricting subject access to data held for purposes of state security, it may not claim the benefit of the Convention in respect of those categories of data. Thus the other Convention signatories may validly impede the transfer of data to or from the United Kingdom where this relates to matters covered by any of the exceptions.

Restrictions may also be imposed upon a transfer to a signatory state where it is considered that this state is acting as an intermediary and that the data will be subject to a further transfer to a non-signatory state.

6.6 Transfer to a non signatory state

The Convention is silent concerning the position of data flows to non-contracting states and the controls which may be imposed upon these. In recent years some attention has been paid to the possible role of contract in ensuring equivalency of protection in respect of transborder data flows. The Council of Europe, in co-operation with the Commission of the European Communities and the International Chamber of Commerce, have produced a model contract which might be used by data users for this purpose. The contract terms are divided into five sections.

The first two sections concern with the obligations of the party initiating the transfer, the licensor, and those of the recipient, the licensee. The licensor is, obliged to ensure that all domestic data protection requirements have been satisfied, whilst the licensee undertakes to ensure that these are complied with in the course of his or her activities. The contract also proposes a number of more detailed obligations which should be accepted by the licensee.

Thus, the purpose for which the data will be used should be specified, there should generally be a prohibition on processing of sensitive data, the data shall be used only for the licensee's own purposes and any errors subsequently notified by the licensor will be rectified immediately upon receipt. Further provisions would hold the licensee liable for any use which may be made of the data and require that the licensor be indemnified in the event of liability arising through the licensee's breach of contract or negligent act. In the event of any

dispute between the parties, the model contract contains provisions for dispute resolution. Reference is made t the possibility that disputes may be submitted to arbitration under the rules established by the ICC or UNCITRAL,.

Finally, provision is suggested for the termination of the contract in the event of a failure by the licensee to demonstrate good faith or to observe the terms of the agreement. Any personal data held by the licensee must be destroyed in such an eventuality. The utilization of contractual techniques may provide what has been described as 'a sort of palliative or complement to the legal framework for data protection and transborder data flow'. There remain, however a number-f objections to their widespread utilization.

A major problem concerns the enforceability of contracts at the suit of an aggrieved data subject. Under the doctrine of privacy of contract, only those who are party to the instrument can rely on it in the course of legal proceedings. It might be, for example, that a data user in England would enter into a contract with a user in the United States under which it is agreed that data will be transferred to the United States with the recipient agreeing to observe all aspects of the data protection principles. In the event the United States' party were subsequently to deny a request for subject access in breach of the principles, although an action for breach of contract may be available to the exporting data user, there would not appear to be any remedy for the data subject.

A more extensive role for codes might be envisaged in states which follow the civil law tradition where third party rights are more readily accepted under a contract:

6.7 Transborder data flows and the directive

Whilst the Convention is effectively silent concerning control of transborder data flows, this topic receives extensive consideration in the Directive. The topic, indeed has been and promises to remain one of the most controversial aspects of the legislation. The Directive's preamble recognizes the dilemmas arising in this area:

> Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals, guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection.

The critical questions are, of course, what might be considered an adequate lack of protection and whether any perceived inadequacies in general legal provisions might be overcome by other sources of rights and remedies In implementing this principle the Directive requires Member States to ensure that:

> . . . the transfer to a third country of data which are undergoing processing or which are intended for processing take place only if . . . the third country ensures an adequate level of protection.

This formulation will require significant changes to the existing United Kingdom system whereby a data user can register an intent to transfer data on a world wide basis and proceed with such transfers unless served with a transfer prohibition notice. The most difficult issue facing implementation of the Directive will concern the determination what is to be considered an adequate level of protection. In this respect it is provided that:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Use of the phrase 'adequate level of protection' clearly does not carry the requirement that the laws of the recipient state conform in every respect with the provisions of the Directive. It would appear unlikely, however, that a total absence of data protection legislation could be regarded as providing adequate protection. As has been discussed earlier, the United States has followed a very different model of privacy protection from that adopted in Europe.

Although proposals have been brought forward for the introduction of a data protection statute, there appears little prospect that this situation will change in the near future. The uniform application of the Directive would clearly be threatened if the decision whether third countries offered an adequate level of protection was to be made by each Member State. It is provided therefore that the Member States and the Commission are to inform each other of any cases where they feel that a third country does not provide an adequate level of protection.

The Directive establishes a Committee chaired by the Commission with membership consisting of representatives of the Member States. In the event that the Commission determines that a third country does not provide an adequate level of protection a proposal for action is to be put to the committee which will reach a decision on the basis of a qualified majority. If the committee endorses the Commission's proposal, Member States will be obliged to take any measures necessary to prevent data transfers to the country involved.

Utilization of this procedure may have the result of establishing a 'black list' of countries to which data transfers will be prohibited. The Directive also provides for the procedures described to be used to identify countries which the Commission considers do provide an adequate level of protection. Given the reference in the Directive to the role of 'sectoral rules' and 'professional rules and security measures' , it is perhaps unlikely that there will be many 'black listings' affecting all data processing activities in a particular jurisdiction. The preliminary drafts of the Directive proposed an absolute ban on data transfers when the recipient country failed to provide an adequate level of protection.

Even allowing for the provisions relating to acceptance of sectoral and professional rules, such an approach would have posed major problems for transborder data flows. As adopted, the Directive modifies this provision to a considerable extent, it now being provided that national implementing statutes may authorize transfers, notwithstanding the absence of adequate protection in the recipient state where:

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment; exercise or defence of legal claims; or the transfer is necessary in order to protect the vital interests of the data subject; or

- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

A number of the issues, not least that concerning the nature of unambiguous consent, are similar to those raised-in relation to the more general aspects of data processing. Others might encompass, for example, the situation where an EU based data subject applies to an EU based credit broker for credit which is to be supplied by a finance company located in the United States.

Assuming that the data subject was aware of the source of the finance, any necessary transfer of data would be authorized under this provision. t is open to Member States to provide for the situations described above in their implementing measures. The indications are that the United Kingdom will seek to make full use of this power. In further derogation from the prohibition against transborder data flows, however, the Directive provides that:

> . . . a Member State may authorize a transfer or a set of transfers or personal data to a third country which does not ensure an adequate level of protection . . . where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

Any exercise of this power must be reported to the Commission and the other Member States. If any party so W formed objects 'on justified measures involving the protection of the privacy and the fundamental rights and freedoms of individuals', a proposal for action may be tabled before the Committee by the Commission and, if approved, will require the Member State involved to take necessary measures to conform. As has been indicated, reliance upon contractual measures poses particular problems within common law jurisdictions, a fact which has been recognized by the Data Protection Registrar.

There appears to be a general acceptance that the volume of transborder data flows is such that it is undesirable for decisions as to acceptability to require table made in the context of individual transfers and that more general provisions should be laid down. The nature of the procedures adopted by the Directive and the open ended prospect that national measures might be challenged at the instance of any other Member State does not seem conducive to

speedy resolution of the issues involved. At a wider level, it maybe questioned how far there is today any realistic prospect of exercising control over transborder data flows.

If consideration is given to the nature of computer networks, of which the Internet is but the largest and best known, concepts such a transfer take a secondary place to the issue of access. Where information is provided on a WWW site it may be a matter of semantics whether the data is accessed by browsers or is transferred to them. Whilst the motives of the European Union in attempting to safeguard the interests of its citizens should be applauded, the contrast may be made between the United Kingdom is overt reference to the fear of data quarantine as a reason for the enactment of the Data Protection Act 1984 and the facility with which countries in the Caribbean and Far East proclaim their status as data havens in seeking to secure inward investment.

If true progress is to be made, the task for the European Union will be to secure the minds of third world countries, persuading them of the need to introduce data protection legislation. It will only be when the subject moves beyond its Western European fiefdom that there will be the realistic prospect of control over global computer networks.

6.8 Short Summary

- The data protection Act Applies to all data users who control the contents and use of personal data from within the U.K.
- The provision of a satisfactory regime must be regarded as one of the major challenges facing international organizations today.
- In the event that signatory state places restrictions on data transfers nothing is impossible usual mechanism exists where by the conformity of this to the convention may be established.

6.9 Brain Storm

- What is means by DBDF?
- How do you transfer data to another convention state?
- How do you transfer data to a non signatory state?

Lecture 7

Information Technology Copyright

Objectives

In this Lecture you will be able to

- Know about Copyright and WWW pages
- About cable programmes and the WWW

Coverage Plan

Lecture 7

7.1 Snap Short

7.2 Provider liability for user misuse

7.3 Newsgroup postings and copyright

7.4 Copyright and WWW pages

7.5 Significant legal issues

7.6 Cable programmes and the WWW

7.7 Copyright in headlines

7.8 Copyright law in Canada

7.9 Short summary

7.10 Brain Storm

7.1 Snap Short

An indication of the relative importance and complexity of the issues involved can be taken from a recent World Intellectual Property Organization (WIPO) estimate that no less than 90% of the total investment in a multimedia product was expended in dealing with intellectual property issues. In its follow-up to the Green Paper on Copyright and Related Rights in the Information Society' the European Commission has estimated that:

> The market for copyright goods and services ranges Community-wide from between 5% and 7% of the GNP This market is comprised of a large variety of products and services, containing protected subject matter ranging from traditional products, such as print products, films, phonograms, graphic or plastic works of art, electronic products (notably computer programs) to satellite and cable broadcasts, CD and video rental, theatres and concert performances, literature and music, art exhibitions and auctioris.

Whilst managing intellectual property rights is very complex and time consuming for those who wish to remain within the law, the ease with which digital information may be copied renders the owners of copyright in literary, artistic and musical works vulnerable to the making and dissemination of unauthorised copies of a work in electronic format. If the invention of the printing press resulted in a move from an oral to a written tradition but at the price of chaining information to the pages of a book, the information revolution frees information in the sense that it may readily be transferred without the need for linkage to paper or any other form of storage device.

7.2 Provider Liability for user Misuse

A related question will concern the service provider's civil liabilities for the making of copies by users of the service or for other acts which may constitute an infringement of copyright. In the United States, a settlement has recently been reached in legal proceedings brought against CompuServe by the owners of copyright in a variety of musical works seeking to hold it responsible for the actions of some of its users who loaded digital copies of musical works onto the service.

Under the terms of the agreed settlement, CompuServe has agreed to make a payment to a copyright licensing agency in return for licenses permitting the future uploading and downloading of copyright works. In an earlier US case Playboy Enterprises v Frena the owner

of a bulletin board was held liable for copyright infringement in respect of photographs uploaded onto the board by subscribers in spite of the fact that he had no actual knowledge of the behavior. As with the issue of liability of service operators for defamatory comments posted on the system, the critical question concerns the degree of control which is exercised over the users and whether the service provider should be regarded as a publisher or merely as a distributor of infringing works.

The question how far a service provider may be held responsible for the activities of its users is of considerable significance for the industry. In the United Kingdom, the decision of the House of Lords in the case of CBS Songs Ltd. v Amstrad Consumer Electronics Plc. is a relevant precedent. The respondents in this case produced audio equipment. Included in their range was a hi-fi unit containing two cassette decks.

This feature allowed a user to copy the contents of one cassette tape onto another, a prospect which caused considerable concern to the owners of copyright in works recorded on cassette, a sector of the audio market which had hitherto enjoyed a considerable degree of immunity from the ravages of home copying. The concern was exacerbated by a further feature which allowed the contents of a tape to be copied in half of the normal playing time.

Action was brought alleging that Amstrad had, by their production of the equipment and the use of marketing strategies described by Lord Temple man as being 'deplorable', 'cynical' and 'open to severe criticism', purported to authorize users to make copies of protected works in disregard of the rights of the copyright owners and in breach of the provisions of the Copyright Act 1956. This contention was rejected by the House of Lords. The critical issue, it was held, was whether equipment could be put to legitimate as well as to illegitimate purposes. Where this was the case, even the most ambiguous marketing strategy could not be regarded as purporting to authorize its use for illegal purposes. 'By selling the recorder', it was held, .'Amstrad may facilitate copying in breach of copyright but do not authorize it'. A similar approach can be seen in the earlier case of CBS Inc. v Ames Records and Tapes where a record library which lent out records and simultaneously offered blank cassette tapes for sale at a reduced price .,as held not to have purported to authorize customers to make infringing copies. A further relevant factor in these decisions was that conduct which might constitute a breach of copyright would take place only after the objects concerned had left the control of the supplier.

A somewhat different situation was at issue in the earlier Australian decision of Moorl2ouse v University of Nezu Soceth Wales, where a university library which made photocopying facilities available to its users was held to have authorized acts infringing copyright when they failed to take sufficient steps to bring the existence of the law of copyright to the users' notice or to supervise the use of the facility to deter would be infringes. As was stated by Gibbs J:

> . . . a person who has under his control the means by which an infringement of copyright may be committed-such as a photocopying machine-and who makes it available to other persons, knowing or having reason to suspect, that it is likely to be used for the purpose of committing an infringement, and omitting to take reasonable steps to limit its use to legitimate purposes, would authorize any infringement that resulted from its use.

It maybe queried whether this dicta is compatible with the extremely restrictive definition of the concept of authorization adopted by the English courts. Assuming that a distinction can be drawn between the situations where a party retains and relinquishes control over equipment used for infringing purposes, the operation of on-line data bases seems to straddle the two concepts.

Physical control over hardware may well be retained by the supplier. This, however, is not essential and there is no reason why portions of a service should not be held on machines controlled by third parties (and even located in other countries) which are linked electronically to the main data base. Users will certainly access the service remotely but it may be argued that the service provider has at least as much possibility of supervising and controlling operations as does a library which makes photocopying facilities available to its users. The issue whether a service provider may purport to authorize users to commit acts which constitute an infringement of copyright may also arise W the context of the practice of those creating World Wide Web pages of including links to other sites which may be of interest to various users.

Assuming that the insertion of a link to another WWW site does not present any legal complications in its own right, the issue may require to be confronted whether the service provider might incur any liability in respect of the contents of the other site. Whilst it would not normally be the case that the publisher of a directory of goods or service providers would e held responsible in the event of any complaint about these, the insertion of on-line links to other service providers might be considered more akin to giving a personal introduction.

LIABILITY OF ISPs

The Internet today has millions of pages and huge collection of information and data. Most of the said data is available for free on the Internet and more than half of the total data on the Net is pornographic material. In addition, there are other data sources available which are directly violative of the intellectual property rights of other entities.

The question that arises for consideration is what should be the liability of an Internet Service Provider (ISP) or Network Service Provider in India for third party information or data made available by him, which has pornographic content, or other data, which violates the intellectual property rights of others. Clause 78 of the Information Technology Bill 1999 states that "no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention".

Thus the normal principle laid down by the IT Bill is that the ISPs are liable for any third party information and data made available by them. However, two wide ranging and loosely drafted exceptions have been given in clause 78. The first exception talks of the personal knowledge of the ISPs. The word used by clause 78 are "his knowledge."

It may be pertinent to note that an ISP doing its business in the normal course of business, would not be aware of any third party information or data being made available by him to his user. The very size of the Internet and the depth of information available on the net makes it humanly impossible for any one including ISPs to have knowledge of the same. It can always be and will be a standard valid defense that the ISP has no knowledge of the offence or contravention.

The second alternative exception provided by clause 78 of the IT Bill is the test of due diligence. If the ISP is able to prove that he had exercised all due diligence to prevent the commission of any of the offence or contravention, he would not be liable.
However, both the exceptions mentioned above, shall be throwing up practical difficulties when the matter would come up in the court relating the production of the evidence of the same. Would a court take whatever an ISP says on its face value and

accept his contention that he had no knowledge of any such commission of offence or contravention? If this be so, then each and every ISP will escape liability. Also, what kW d of evidence, barring oral evidence, will an ISP lead in a court of law to prove that he had no knowledge?

Another related issue is what kind of evidence would be produced by the prosecution or the plaintiff to prove that the ISP had knowledge of the commission of the said offence or contravention? The adjudication of the said issue will raise some very ticklish legal issues. Another issue that would arrive for adjudication is whether the ISPs are expected or presumed to have knowledge of everything and anything made available on the Internet which the ISP is providing to the user. `

The second exception raised by clause 79 again raises the peculiar issue what could be "due diligence" when we talk of Internet and Cyberspace. No firewall or filter in the world is absolute or unbreakable. As such, we are in the changing sands of emerging technologies and standards, Cyberlaw would be called upon to decide what could be "due diligence" that could be expected of an ISP to prevent the commission of any offence or contravention. How can an ISP sitting in his office get to know whether any person is about to commit any Cyber offence? Seen from one extreme angle, every citizen is a potential Cyber criminal and no mount of diligence, of whatever extent or nature, can be termed as due diligence.

Recently, an American court has delivered its judgment which reiterates the principle that the ISP is not liable for third party information or data.

Globally, it is being strongly felt that the interests of the copyright school have to be balanced arid safeguarded. Cyberlaw on the said issue is still emerging.

Source: Pawan Dugal, Liability of ISPs, Economic Times, 20th May, 2000.

In the United Kingdom, for example, statutory and other official information is protected under the law of copyright. In other jurisdictions this is not the case. Copies of UK statutes can be found on Internet sites in third countries and it might be argued that a UK provider who publishes a link to such a site could incur liability on the basis of inciting a breach of copyright in the event that users followed the link to obtain an infringement of copy of the

statute. The issue of incitement was raised in the case of CBS Songs Ltd. v Amstrad Consumer Electronics plc. Although it was accepted by Lord Templeman that a defendant who procures a breach of contract is liable jointly and severally with the infringer for the damages suffered by the plaintiff, he went on to hold that the decision to make infringing copies was one which was made by the customer subsequent to the acquisition of the machine. `Generally speaking' he ruled:

> . . . inducement, incitement or persuasion to infringe must be by a defendant to an individual infringement and must identifiably procure a particular infringe in order to make the defendant liable as a joint infringer.

In the situation where a site provider inserts a link to a specific document communication to another site, the fact that connection is being made to another site in another country may not be apparent to the user. Given that the mere act of viewing a document on the Web will entail its reproduction, it is submitted that the insertion of a direct link would suffice to establish liability The provision of a less specific link, however, to a site upon which the user might find material which could be copied in infringement of copyright would not satisfy the criteria laid down by Lord Temple man.

7.3 Newsgroup Postings and Copyright

The recent and controversial introduction of the Microsoft Network has prompted the adoption of an interesting legal technique by some posters to Usenet newsgroups. These postings are also carried by a substantial number of commercial service providers including the Microsoft Network Providing access involves the service provider making and holding copies of newsgroups (an issue discussed further below).

Messages similar to the two reproduced below are now appended to some postings: Microsoft Network is prohibited from reproducing this work, in whole or in part. Copyright 1995, xxxx. License is available to Microsoft Network to reproduce this work for $1000. Unauthorized reproduction by Microsoft Network constitutes breach of agreement to these terms. '

Microsoft Network is prohibited from reproducing this work in any form, in whole or in part, without the express written consent of the original author. It is uncertain to what extent such

techniques, which clearly are intended to hinder the operation of the Microsoft network, will be effective. There would appear to be no practicable mechanism for a service provider such as Microsoft to read all Usenet postings and remove those with conditions similar to that described above. It may be that persons objecting to the reproduction of their messages on the Microsoft network could contact Microsoft with the warning that reproduction was prohibited.

Even in this event, although it might be possible to operate a 'kill file' which would suppress all messages originating from a particular poster, other features and conventions of the Usenet system may make enforcement impractical. It is common practice on electronic newsgroups for posters to copy all or part of a previous message in making a reply or rebuttal. In part this is desirable because of the dispersed nature of the newsgroup. This can mean that the reply to a message may appear on some sites before the original posting.

Failure to quote from the original would make the reply even less comprehensible than is the norm with newsgroup postings. There could be no guarantee, therefore, that a message from a reluctant poster would not appear in the body of a message from another user. As discussed above, the contents of a newsgroup are copied by every service provider carrying them. The normal operation of Usenet involves a single message being copied several thousand times.

The argument is often made against the licenses (and exclusion clauses) which software producers seek to impose on purchasers, that the terms are brought to the attention of the user too late to be validly incorporated into the contract. Use of a software program will require its reproduction but the argument appears to be accepted that a lawful acquirer of software could rely at least upon an implied term of the contract allowing its use. This argument might be turned against the user in this case, the argument being that a Usenet poster impliedly consents to the reproduction of the work and that the restrictive notice appears too late to be effective.

It is almost as if a person submitting a letter to the correspondence columns of a newspaper attempted to impose restrictions upon the range of dissemination of copies of the paper. In this situation, of course, the decision whether the letter should be published is one for the newspaper. Publication, however unlikely a prospect, may be seen as acceptance of the writer's condition. With immoderate newsgroups, there is no intermediate stage between submission and publication.

7.4 Copyright and WWW pages

In October 1996 a judge in the Outer House of the Court of Session in U.K. was asked to grant an interim interdict (temporary injunction) preventing one 'on-line newspaper' providing links to another on the grounds that such conduct constitutes a breach of copyright. The case of Shetland Times Ltd. v Dr Jonathon Willis is the first of its kind to come before a court in the UK. Although it is important to stress that the court was asked merely to decide whether the linkage should be stopped, pending a full trial of the issues, the novel nature of the action makes it of some interest and possibly significance.

7.5 Significant Legal Issues

The pursuer's case was based upon two lines of argument. First, it was argued that the pursuer's WWW site constituted a 'cable programme service' within the meaning of the UK's Copyright, Designs and Patents Act. This statute provides further that 'any item included in a cable programme service' is to be classed as a 'cable programme'. It was argued that the headlines made available on the Times web site constituted such a programme.

The defenders system would have the same status and section 20 of the Act and the unauthorized inclusion of the pursuer's material would constitute an infringement act. The second argument advanced was to the effect that copyright subsisted in the Times headlines as literary works and that their, reproduction on the News site constituted an. infringement.

7.6 Cable Programmes and the WWW

The classification of Web sites as cable programme services might be a matter of some significance to operators. Section 7 of the Act defines a cable programme service as:

> . . . a service which consists wholly or mainly in sending visual images, sounds or other information by means of a telecommunications system, otherwise than by wireless telegraphy for reception

Interactive services will, therefore, be excluded from the definition of cable programme services although it has been argued that electronic databases might be classed as cable

programme services. For the defenders, it was argued first that www sites should not be classed as cable programme services as the processes involved in their operation did not involve 'sending' information. Rather, it was suggested, the information was made available for collection by users of the site.

The site operated 'entirely passively'. It was also argued that WWW sites fell within the scope of this exception. Particular reference was made to the feature which is invariably provided enabling users to send e-mail to the site operator. Neither of these arguments was accepted by the judge. The fact that the transfer of information required to be initiated by the user did not prevent it being sent by the service provider. This view, it is submitted, is surely correct.

Although most cable programmes currently provided operate at the level where a programme is broadcast at a specific time with users simply choosing whether to view it or not, the statutory definition clearly envisages a system such as 'video on demand' when viewers will be able to select the time at which they wish to view a particular programme. The transfer of information would not be possible but for the provision of the necessary facilities by the web server owner.

The issue whether the operations of WWW sites should be considered interactive raises more significant and complex issues which were not considered at any level of detail. Argument before the court proceeded by reference to the possibility that a user could send an e-mail to the site operator. This it was considered was not an essential element of the service. Additionally, it was held, the e-mail feature could be separated from the cable programme aspects of the service. More interesting issues might have been raised (and may be raised in the event that the case proceeds to trial) concerning the whole nature of WWW operations.

A considerable amount of information is transmitted from a user's computer whenever a site is accessed. This will be even more so in the event that a site operates a registration system. Devices such as 'cookies' may also add to the interactive aspects of the WWW. Although it might be suggested that the information is sought for the 'operation or control' of the service in many instances the information may be sought for other purposes such as marketing. Although the arguments presented were considered sufficiently substantial to persuade the judge that an arguable case of infringement had been made out and that the interim interdict sought should be granted, it may be that more extensive consideration will reveal the cable programme arguments to be flawed.

Although superficially attractive in the context of particular forms of WWW sites, technological developments seem to be making the classification less appropriate. It would be a source of considerable confusion if some WWW sites were t be classed as cable programme services whilst others, perhaps because of the use made by the owner of information generated by users, were to be excluded from this category.

7.7 Copyright in headlines

A further issue which was not raised in the interim proceedings concerned the question whether the headlines of stories should be considered as constituting a cable programme in their own right. Although the statutory definition classes 'any item included in a cable programme service' as a cable programme it appears unrealistic to separate the headlines of a newspaper story from the underpinning text. If the entire story were to be classed as the 'item' then the issue to be determined will be whether the headline itself constituted a 'substantial' part of the protected work.

The issue of the copyright status of headlines was discussed more directly in the context of the second part of the pursuer's claim, alleging that these should be classed as literary works so that their reproduction by the defenders would constitute breach of copyright. Although the case of Exxon Corpn. v Exxon Insurance Consultants Ltd. is authority (albeit English) for the proposition that copyright does not subsist in a single invented word, it is unclear how much more is required for its protection. Given the low qualitative threshold applied in the UK there is no reason in principle why a newspaper headline should not be regarded either as possessing copyright in its own right or being considered as a substantial part of the accompanying story. In the nineteenth century case of Lamb v Evans the headings (presented in English, French, German and Spanish) in an international trade directory (somewhat akin to the modem 'Yellow Pages' type directories) were held to be protected by copyright. Many of the headings used were extremely short, 'Absinthe' and 'Brush Manufacturers being two examples cited in the law report. It would appear from the judgment that the protection was extended to the totality of the headlines rather than to individual examples.

Some of the pursuer's headlines, it was indicated; w ere around eight words long. In one of the few decisions concerned with the issue, it was held in the case of Francis, Day and hunter

Ltd. v Twentieth Century Fox Corpn. that no copyright subsisted in a song title, 'The Man Who Broke the Bank in Monte Carlo'. The Privy Council held that:

As a general rule, a title is not by itself a proper subject-matter of copyright. In certain circumstances, it was recognized titles might display sufficient literary merit to be deserving of protection in their own right but in this case:

> There may have been-a certain amount, though not a high degree, of originality in thinking of the theme of the song and even in choosing the title, though it is of the most obvious. To 'break the bank' is a hackneyed expression, and Monte Carlo is, or was, the most obvious place at which that achievement or accident might take place.

Given the frequency with which competing newspapers use identical headlines without any suggestion of copying, it is clear that the same comments could be applied in this context. The example cited above alleging errors on the part of a council would appear an obvious example, the epithet 'cock up' being as commonplace in media reports of mal administration as is the notion of breaking the bank in financial matters.

7.8 Copyright law in Canada

COPYRIGHT LAW IN CANADA

Canadian copyright law is governed by the Copyright Act, which protects original literary, artistic, musical and dramatic work5. A partial list of works which are entitled to copyright protection in Canada includes: books, newspapers, dictionaries, manuals, catalogues, magazines, pamphlets, computer software, paintings, drawings, design trade-marks, sculptures, architectural works, engravings, dramatic works, photographs, films, videos, scripts, maps, lyrics and musical works.

One very significant right granted to the owner or ' Canadian copyright iii a work, is the exclusive right to reproduce the work, (or any substantial part of the work) in any material form whatever.
For example, the owner of copyright in a book ha s the , right to stop others from making copies of the books, (or any I substantial part of the book), whether the copying is by way of a computer image/text scanner.

In addition to acquiring the exclusive right to copy the work, the owner of copyright in

a work also receives an entire "bundle" of rights, some of which are specific to the type of work in question. For example, in the case of dramatic work, copyright includes the right to convert the dramatic work into a novel. In the case of computer software, it includes the right to rent the software to others. Each different type of work has its own bundle of copyrights.

Copyright comes into existence automatically, at the time the work was created, and, in the case of most works, it continues until the end of the calendar year in which the author of the work dies (regardless of whether the author has sold or i assigned the copyright into he work or not), and continues for an additional period of 50 years. There are some notable exceptions of this rule however. One such exception relates to photographs, which are protected by copyright from the time the photograph was taken up, until the end of the calendar year in which the photograph was taken, and for an additional period of 50 years (that is, the termination date of copyright ; protection for photographs is linked to the date the photographs was taken, and not the date of the ' photographer's death).

"Moral" rights are also protected under Canadian copyright law. Moral rights include the author's right to be j associated with the work by name, or pseudonym and the ; right to remain anonymous, and include the author's right to the integrity of the work (that is,
the author's right to stop the work from being distorted, mutilated or modified, to the prejudice of the author's honor or reputation, or from being used in association with the product, service, cause or institution).

Moral rights remain with the author of a work, even where the work, or the copyright in the work, has been sold or assigned. Moral rights continue to exist in a work for the same length of time as other copyrights in work in question.

7.9 Short Summary

- Breach of copyright would take place only after the objects concerned had left the control of the supplier.
- Uk's copyright , design and patents Act provides any item included in a cable programme service.
- Copyright comes into existence automatically at the time the work is created.

7.10 Brain Storm

- Discuss about Newsgroup postings.
- Give Note on Copyright and WWW pages.
- Describe Cable Programmes and the WWW
- Explain the copyright Law in Canada.

Lecture 8

Nature of Copyright Protection

Objectives

In this Lecture you will learn the following

- Right to copyright owner
- Literal and non-literal copying
- Willful ignorance
- Error correction
- Reverse Engineering and de-compilation
- Public performance Adaptation and translation
- IRP in software
- How to be copyright protected
- Legal action.

Coverage Plan

Lecture 8

8.1 Right to copyright owner
8.2 Substantial similarity
8.3 Literal and non-literal copying
8.4 Justifiable similarities
8.5 Unconscious copying
8.6 Willful ignorance
8.7 Fair dealing
8.8 Error correction
8.9 Back up copies
8.10 Reverse Engineering and de-compilation
8.11 Reverse Engineering and computer programmers
8.12 Other infringing acts
8.13 Issue of copies to the public
8.14 Public performance
8.15 Adaptation and translation
8.16 Moral rights
8.17 Resale and rental of copies of a protected work
8.18 Computer programmes as audio or visual works
8.19 Digital sampling
8.20 Computer programmes as photographs or films
8.21 IRP in software : An Indian perspective
8.22 How to be copyright protected
8.23 Legal action
8.24 Short Summary
8.25 Brain Storm

8.1 Snap Shot

There are several mechanisms for copyright protection among them, the award of a patent serves to confer upon the successful applicant a monopoly in respect of the exploitation of its subject matter. Although judicial references have been made to copyright conferring a monopoly-in the case of Green v Broadcasting Corpn. of New Zealand Lord Bridge, delivering the judgment of the Privy Council, stated that the protection which copyright gives creates a monopoly'-the copyright owner possesses only the exclusive right to perform certain acts in respect of the work.

RIGHTS OF COPYRIGHT OWNER

These comprise the rights:

- to copy the work or any substantial part of it;
- to issue copies of the work to the public;
- to perform, show or play the work in public;
- to broadcast the work or include it in a cable programme service; and
- to make an adaptation of the work or do any of the above in relation to an adaptation.

In respect of computer programmes, it is provided that in respect of a computer programme, adaptation 'means an arrangement or altered version of the programme or a translation of it'.

If a party possesses the exclusive right to perform an act, it follows that any other party attempting that act will be guilty of infringement. In most situations, infringement of a copyright will expose the perpetrator to a civil action brought by the copyright owner, but the legislation also establishes a number of criminal offences which may be committed by those engaged in the production or supply of infringing copies for commercial purposes. For the purposes of the present study, the most significant infringing act is that of copying the work. The act of copying is defined as involving the reproduction of the work, or a substantial part of the work in any material form. This is to include 'storing the work in any medium by electronic means'. Thus, for example, the use of some form of scanning device to transform text into electronic format will constitute an infringement of copyright. As was stated by Whit ford J in LB (Plastics) Ltd. v Swish Products Ltd., the law of:

> ... designs and patents give a monopoly effective against persons whose work owes nothing to the work of the design proprietor or the patentee. In these cases there is a true monopoly. From start to finish, copyright never stops anyone working on the same lines, upon the same sort of basic idea, and copyright cannot be effective against anyone who produces something independently

8.2 Substantial Similarity

As stated above, infringement of copyright does not require that an exact copy be made of the whole of a work: Copying of a substantial portion will suffice. The identification of what may be regarded as a substantial portion contains quantitative and qualitative elements.

Although not without its problematic areas, the quantitative element is of limited significance. Clearly, a party cannot copy 99,999 words from a work of 100,000 words and put forward the defense that the work has not been copied in its entirety. Equally, it may be difficult for the copyright owner to allege that the quotation of a 100-word passage from the work constitutes a substantial part.

In between these lies the Grey area where consideration is addressed primarily to the qualitative significance of the portion copied to the total work. In cases on this point, the courts have concerned themselves largely with the economic consequences of the activity. If the portion copied can be regarded as constituting a significant portion of the work's value to the copyright owner, infringement may be found even though it constitutes a relatively small portion of the whole. In the case of a computer programme, for example, the novelty and value may lie in one routine which constitutes a comparatively small portion of what is otherwise a fairly standard programme. Here, copying of the routine might well be regarded as an infringement of copyright.

8.3 Literal and non-literal copying

Copying must involve a degree of intention on the part of the copyist. In demonstrating the operation of probability theory the statement is sometimes made that 'if you give enough monkeys enough typewriters, sooner or later one of them will reproduce the collected works of Shakespeare'. Disregarding the inconvenient fact that the works of Shakespeare are no longer protected by copyright law, the production of such a work would not involve any

infringement of copyright as no element of copying would be present. Such a result serves to illustrate a significant difference between the patent and copyright regimes.

In the former case, the fact that infringement occurs innocently provides no defense. In the case of computer programmes, claims of copyright infringement fall into two categories. The first, and considerably the simpler, concerns the situation where there is evidence of similarity at the level of the code and comes under the heading of literal copying. At the most blatant level this will constitute what is frequently referred to as 'software piracy where illicit copies of software packages are made with a view to being distributed and sold. A recent study conducted by the Business Software

Alliance and the Software Publishers Association and covering the years 1994 and 1995 estimated that the losses to the industry amounted to $12.2 billion in 1994 and $13.3 billion in 1995. In many countries the quantity of pirated software exceeded the number of legitimate copies. In Vietnam, for example, it was estimated that 99% of software was pirated, with the figure for China being 96%. Even in Western Europe, 86% of software in Greece was considered to be pirated, 51% in France, with the UK being the most law abiding country with a figure of 38%. For the United States the figure of software piracy was 26%.

In financial terms, the losses to producers in the UK were put at almost half a billion dollars. Other surveys have produced broadly similar results. As with figures relating to the scale of computer fraud, any estimates are dependent upon the assumptions underlying the study. The BSA/SPA figures cited were derived by calculating the volume of hardware sales and making an estimate as to the number of software packages normally required by users in the business and consumer sectors.

The unknown factor, of course is whether, assuming piracy could be eliminated, those making use of pirated copies would purchase legitimate copies. It might even be argued that reducing software piracy might have a detrimental effect on hardware sales as purchasers give consideration to the question whether they can afford to pay the full price for software? From a legal perspective there is no doubt that the complete reproduction of software packages will constitute an infringement of copyright. In other cases elements of an earlier work may be reproduced.

A typical scenario will see an employee changing jobs and subsequently producing software which incorporates routines from earlier works, the copyright in which will, of course, vest in the original employer. The issues involved here essentially concern the questions whether a

substantial amount of the previous work has been reproduced and whether any similarities can be explained by reasons other than that of deliberate copying.

An illustration of such a situation can be found in the case of IBCOS Computers Ltd. v Barclays Mercantile Highland Finance Ltd. Here, the first defendant had been employed by the plaintiff on the development of a software product intended for use by agricultural dealers which was marketed under the name ADS. On leaving its employment, he developed a further and competing product which was marketed under the name of Unicorn.

The plaintiff alleged that sufficient features of this were copied from the original to constitute an infringement of copyright. In determining the criteria which would be applied in determining the question whether infringement had occurred, Jacob J held that the court should determine whether there was a sufficient degree of similarity between the two works which, coupled with evidence of access to the original work, would establish an inference of copying.

The onus would then switch to the defendant to establish that the similarities were explicable by causes other than copying. Evidence that 'functional necessity' served to narrow the range of options open to the defendant would be relevant. Trivial items may well provide the most eloquent testimony. As was said in Billhofer Maschinenfabrik GmbH v TH Dixon F Co. Ltd.

It is the resemblance in inessentials, the small, redundant, even mistaken elements of the copyright work which carry the greatest weight. This is because they are the least likely to have been the result of independent design. In the present case, evidence was presented that the same words were misspelt in the same manner, the same headings were used in the two programmes and both shared the same bit of code which served no useful purpose for the functioning of the programme. Beyond this, there were considerable similarities at the level of the code itself. In respect of one element of the programmes it was held that:

> . . . there are 22 identical variables, 8 identical labels, 1 identical remark, 31 identical code lines and one identical redundant variable. This to my mind plainly indicates copying and enough in itself to constitute a significant part.

The court recognized in an another case that copyright protection must extend beyond the literal aspects of the programme code to aspects of 'programme structure' and 'design features'. In the case of the former element, it was held that copyright subsisted in the

compilation of individual programmes which made up the ADS system. Although some differences existed between ADS and Unicorn it was held that the defendant had taken `as his starting point the ADS set and that set remains substantially in Unicorn .

Although the two programmes had a different visual appearance and it was recognized that 'Unicorn is undoubtedly to the user a much friendlier programme than ADS was at the time', the defendant, it was held had taken 'shortcuts by starting with ADS and making considerable additions and modifications'.

8.4 Justifiable Similarities

In any dispute, it will be a question of fact whether a later work has been copied from an earlier. This may be no simple task. In civil cases the standard of proof applied refers to the balance of probabilities. Given this, it must be unlikely that a party responsible for the production of an exact copy of a work could establish that this was entirely serendipitous. The task of determining the issue will be more complex in the event that the later version is not an exact copy of the original.

Particularly in the case of computer programmes, a variety of producers may be operating in the same field. In such a situation, and especially given the technical constraints which may operate, close similarities between two works may occur in the absence of deliberate copying or plagiarism. Similarities in the educational background of different programmers might also result in the production of substantially similar portions of programme.

8.5 Unconscious Copying

A further point of considerable relevance raises the possibility that a party may have retained knowledge of a work in his subconscious with this serving to influence the format of the later work. The case of Seager v Copydex Ltd. provides an excellent illustration of this situation. Here details of a new design of carpet fastener were submitted by the plaintiff to the defendant.

The fastener had been given the name 'Klent' and the plaintiff held a patent in respect of its design. The submission was made at the defendant's request. Negotiations continued between the parties for a period of more than a year but came to nothing. During the course

of these negotiations, the plaintiff volunteered to the defendants information regarding a second form of carpet grip.

Shortly after the end of the negotiations, the defendants marketed a carpet grip, very similar in design to the plaintiffs second suggestion. It was given a name, 'Invisgrip', similar to that suggested by the plaintiff ('Invisgrip') was patented by the defendants and achieved considerable commercial success. The plaintiff subsequently claimed that the defendants must have used the information which he had given to them in the course of negotiations and that this was a breach of confidence. Much of the evidence before the court concerned the nature of these negotiations and the circumstances in which the information was divulged to the defendants.

The plaintiff contended that there had been clear and unambiguous reference to the second design and that he had handed over preliminary sketches to the defendants. The defendants' evidence was to the effect that the possibility of the plaintiff supplying a modified design had been mentioned only briefly and had been dismissed by them out of hand. By the end of the negotiations the defendants had formed the view that the plaintiff was acting in an 'evasive' fashion and that it would be impossible to do business with him. They accordingly determined to proceed with the marketing of a carpet fastener on their own account. To this end they took advice as to the validity of the plaintiff's patent and as to the extent to which their discussions might inhibit their freedom of action.

Acting upon this advice they produced an amended version of the 'Klent' design. This was intended to avoid the plaintiff's copyright but replicated key features of his second design. The plaintiff argued that this resulted from the misuse of the confidential information supplied to the defendants. They countered that their alternative grip was the product of their own ideas and owed nothing to the information supplied by the plaintiff. In the Court of Appeal; Lord Denning MR stated the facts broadly as recited above and concluded that:

> I have no doubt that Copydex honestly believed that the alternative was their own idea, but think that they must unconsciously have made use of the information which Mr Seager gave them. The coincidences are too strong to permit of any other explanation.

The issue of unconscious copying has also arisen in a number of cases concerned with musical works. A further situation may arise where an employee leaves one position only to engage in similar work. Where both jobs entail the production of copyright protected work; it may be very difficult to erase all knowledge of the original employer's work. An example of such a situation is seen in the case of John Richardson Computers Ltd. v Flanders (No 2).

8.6 Willful Ignorance

A further aspect of this topic which is of special relevance to information technology concerns the extent to which a party may be deliberately ignorant of the existence of an earlier work. The use of so-called 'Clean Room' technique, attempts to ensure that employees responsible for the design of components which are likely to be similar to those of a competitor are kept in ignorance of the earlier work. Whilst it is the case that a generally independent creator has nothing to fear from the la. of copyright, where work is conducted on behalf of a third party, the nature and extent of any instructions given will be significant in determining whether infringement has occurred.

Acts permitted in relation to protected works ' Although the Act reserves a number of rights to the owner of copyright, it must always be remembered that intellectual property rights constitute exceptions to the general prohibition against acts which are restrictive of competition. As such, any acts which are not prohibited will be permitted.

Additionally, the Act makes references to a number of actions which would normally constitute an infringement of copyright but which may, in certain prescribed situations, be lawfully carried out. The range of permitted acts has been extended as a result of the implementation of the provisions of the Directive on the legal protection of computer programmes.

8.7 Fair Dealing

Undoubtedly the best known of the statutory exceptions is that which permits 'fair dealing' with a protected work for the purposes of research or private study. Few of these expressions receive any form of definition in the legislation. The concept of 'fair dealing' will undoubtedly permit a degree of copying of a protected work, but the supplementary question, 'how much?' cannot be definitively answered. At one time the UK publishing industry suggested that the copying of up to 10% of a book might be regarded as a fair dealing. This was, however, an informal indication which was subsequently withdrawn.

It would not appear that the extent of copying permitted under this heading has been at issue in any case. Whilst the concept of private study is not one which will be of great practical significance in the software field, that of research is potentially much more so. It is to be noted

that the word 'research' precedes the phrase 'private study in the Act. It ' would appear to follow therefore that its application is not restricted to the area of individual research but will also extend into the commercial sphere. In the case of a traditional literary work such as a book or an article the acts which encompass fair dealing can readily be identified.

Clearly, researchers must be able to read the work and to quote small portions of it in any work which they themselves might compile. In the course of this task they may cop portions of the work, perhaps by means of a photocopier, although infringement may occur equally well if the work is copied by hand. It must be accepted that the concept of fair dealing in a literary work cannot extend to the making of a copy of the complete work. Different considerations may apply in respect of software. Two arguments can be put forward in support of such a proposition.

First, whilst it is a very simple task to copy portions of 1 book, indeed it is much easier to copy a part than the whole, the reverse is the case with respect to a computer programme. A second argument operates at a utilitarian level. The user of book would generally be considered as having no legitimate need to take a second copy of the work in case the original suffers damage. This view would be justified on the basis that although the cosmetic appearance of a book may easily be harmed, e.g. through the spillage of a cup of coffee, the damage will seldom be such as to prevent its continued use. Software is a much more fragile creature and, especially if research is being conducted as to its make-up, terminal damage may easily result. In such an event the making of a back-up copy might appear a reasonable precaution. In concluding the examination of the fair dealing exception the point must be stressed that any of the actions referred to above will. be sanctioned only to the extent that they are carried out in connection with research.

It is specifically provided that recompilation of a programme will not be permitted under the fair use provisions. Assuming that a copy of software may legitimately be made for research purposes, its status will change in the event that the research ends and the copy is put to operational use.

8.8 Error Correction

It is received wisdom that every, computer programme contains errors or 'bugs'. In accordance with the requirements of the European Union Directive, it is provided that an authorized user may copy or adapt a programme 'for the purpose of correcting errors in it'.

This Provision might appear to give a user carte blanche to copy a programme in the quest to discover errors. An alternative, and perhaps preferable view, is that the right will extend only in respect of particular errors which have been discovered by the user in the course of running the programme in a normal manner. Even on this basis, uncertainties remain as to the extent of the user's rights.

Computer programmes are not like other literary works. A typing or grammatical error occurring in a book may be corrected without the act having any impact upon the remainder of the wok. The relationship between the various elements of a computer programme is much more complex. If an error is discovered in the course of running a programme, its cause may lie almost anywhere in the programme. If the source of a particular error is detected and a correction made, it cannot be certain that the effects of the change will not manifest themselves in an unexpected and undesirable fashion elsewhere in the programme.

There is indeed a school of thought in software engineering that suggests that when errors are detected, rather than amending the programme, operating procedures should be changed to avoid the conditions which it is known cause the specific error to occur.

8.9 Back-up Copies

Computer programmes are invariably supplied on some storage device such as a disk or tape. Such storage media are notoriously fragile and it is all invariably possible that their contents might be accidentally corrupted or erased. In such circumstances it might not appear unreasonable for a user to seek to take a second or back-up copy of the work with the intention that this will be stored in a safe location and brought into use in the event that the original copy of the software be destroyed. As enacted, the United Kingdom Act (in contrast to several other copyright statutes) made no mention of the possibility that a user might make a back-up copy of a programme which had been lawfully acquired.

Although, once again, it is possible to argue that such a term must be implied into any relevant contract, the argument is more tenuous than that relating to the implication of a basic use right. Implementation of the provisions of the Directive has brought about a measure of reform, the Act now providing that a back up copy may be made by a user where this is necessary . . . for the purposes of his lawful use'. It is unclear how useful this provision might be. The making of a back-up copy will invariably be a wise precaution but it is difficult to

conceive of any situation where the presence of a second copy is 'necessary' for the functioning of the original.

Some small measure of consolation may be offered to a user by the fact that the copyright owner may not validly restrict or exclude the operation of the provisions regarding the making of back-up copies. It is doubted, however, whether the new provisions will alter significantly either the la, or the practice in this area.

8.10 Reverse Engineering and De-Compilation

When software is supplied to a customer, it will be in a form known as object or machine-readable code. If this were to be viewed b a user it would appear as a series, a very long series of zeros and ones. Obtaining sight of these digits will give little indication as to the manner in which the programme is structured. Although it is possible for a programme to be written in object code, much more programmer friendly techniques are available and almost universally utilized.

A number of what are referred to as 'high level' languages exist- examples are BASIC and FORTRAN. These allow programmers to write their instructions in a language which more closely resembles English, although the functional nature of computer programmes limits the variations in expression which are a hallmark of more traditional literary works. Most users, of course, will be concerned only with what a programme does rather than the manner in which this is accomplished. Some, however, may have different motives.

The practice of reverse engineering has a lengthy history in more traditional industries and typically involves the purchase and dismantling of the products of a competitor. In the computer context, reverse engineering may involve study of the operation of a computer programme in order to discover its specifications. This is essentially a process of testing and observation and might involve pressing various keys or . combinations of keys in order to discover their effects. The 'technique known as recompilation may be used as part of this process. Normally involving the use of other computer programmes to analyze the object code, the technique seeks to reproduce the original source code.

Although in the LB Plastics case the alleged infringes had obtained a degree of access to the product drawings, in neither case was it argued that these had been reproduced directly;

instead the case was based on the contention that by reproducing the finished object, respectively furniture drawers and a vehicle exhaust system, the provisions of Section 48(1) of the 1956 Copyright Act had been breached. This provided, inter alia, that copyright in a two-dimensional work, the product drawings, will be infringed by converting these into a three dimensional form, the product.

In LB (Plastics), the plaintiff designed and produced a drawer system. The key feature was that the drawers could be supplied to customers (generally furniture manufacturers) in what was referred to as 'knock-down' form. This offered considerable benefits at the transportation and storage stages whilst the design facilitated swift and easy assembly of the drawers by the final producer.

The concept proved commercially successful and some time later the defendant introduced a similar range of products. It has alleged that this was achieved by copying one of the plaintiffs drawers. In the High Court, Whit ford J accepted that the resulting product infringed the plaintiff's copyright in two of the original product, drawings. Although this ruling was reversed by the Court of Appeal, which held that an insufficient causal link existed between the drawings in question and the defendant's product, it ,as reinstated by the House of Lords. '

A significant factor underpinning the judgment would appear to have been the recognition that although the defendant was required by commercial dictates to ensure that its drawers were functionally compatible with those produced by' the plaintiff, this could have been attained in ways which required less in the way of replication of the original design. The decision in LB Plastics was approved in the subsequent case of British Leland Motor Corporation z Armstrong Patents. Here, the plaintiff manufactured motor vehicles. The multitude of parts which make up each vehicle were produced in accordance with detailed designs drawn up by the plaintiffs.

The defendant specialized in the manufacture of spare parts, in the particular case an exhaust system which would be offered for sale to motor vehicle owners. In order to allow the replacement systems to be fitted to the plaintiff's vehicles their design required to be virtually identical to that of the original component. This was achieved by taking an example of the plaintiff's exhaust system and examining its shape and dimensions.
The plaintiffs exhaust system was not itself eligible for copyright protection; neither was protection available under the law of patents or of registered designs. The court's attention

was directed therefore to the question whether copyright subsisted in the original engineering designs and, if so, whether the defendant's conduct constituted an infringement. Holding in favour of the plaintiff on the issue of copyright infringement, the court (Lord Griffiths dissenting on the basis that although the majority's opinion was in line with precedent, the case was one which justified the application of the 1966 Practice Direction) held that the defendant's conduct amounted to indirect copying of the designs, constituting a breach of Section 48(1) of the Copyright Act 1956. This provides that the conversion of a two dimensional work into one of three dimensions will constitute reproduction.

A further relevant case on this point is that of PIix Products Ltd. z Frank M Winstone, a case heard- before the High Court of New Zealand whose decision was upheld on appeal to the Privy Council. This case concerned the design of containers designed for the transport of Kiwi fruits. During the 1960s and 1970s, the plaintiff designed and produced a number of containers which offered significant advantages in respect of the safe storage and transportation of the fruit.

8.11 Reverse Engineering and Computer Programmes

Computer programmes can be divided into two broad categories-operating systems and application programmes. An operating system, the best known examples of which are perhaps MS DOS or Microsoft Windows, contains the basic instructions necessary for a computer to operate. A very simple analogy might be made with a railway system. The gauge of the track and the height and width of tunnels and bridges night be regarded as equivalent to an operating system.

They set down basic parameters which must be respected by anyone wishing to build a train to operate on the system. If the track gauge is 4ft. 8ins, no matter how, technologically advanced an engine might be, it will be quite useless if its wheels are set 7ft. apart. In the computer field, programmes such as word processing and spreadsheet packages constitute the equivalents of railway engines. They work with the operating system to perform specific applications and must respect its particular requirements.

A producer intending to develop an applications package for use on a particular operating system must be aware of its functional requirements. In most instances, the information necessary will be made available by the producer of the operating system whose own

commercial interests will be best served by the widest possible availability of applications to run on the system. In the event that the information is not readily available-or that it is suspected that only partial information has been made available-the attempt may be made to reverse engineer the operating system. A second occasion for the use of reverse engineering occurs at the level of applications packages.

Programmes such as word processors and spreadsheets store data in a particular format. In the case of basic text, a widely used standard exists called ASCII (American Standard Code for Information Interchange). The text of most word processed documents is a much more complex creature.

Particular fonts, type size and line spacing will be used. Portions of the text may be printed in italics or may be emboldened or underlined. These matters are not standardized. A producer intent on developing a new word processing programme, may wish to discover the codes used by rival producers so that conversion facilities may be built into the new product. From a commercial perspective, existing users are more likely to change to a new programme if they can still use documents created using their existing programme.

The final form of reverse engineering is the most controversial. Here, the object of the reverse engineering is to discover information about the user interface of an applications package which may then be used as the basis for the attempt to produce a substantially similar package. In early court cases on the point in the United States it was often asserted that the intent was to reproduce the 'look and feel' of the original package.

8.12 Other infringing Acts

Although the act of copying all or a substantial part of a protected work might constitute the most significant form of infringement, a variety of other forms of behavior are also prohibited and may be of some relevance within the information technology context.

8.13 Issue of copies to the Public

The owner of copyright in a work has the right to determine whether copies of that work might be made available to the public. This right extends only to the first occasion upon which the work is made available and not to any subsequent dealings in the work by way of importation, distribution, sale, hire or loan. It is provided, however, that the rental of the work is to constitute a restricted act.

8.14 Public Performance

The acts of performing or showing the protected work in public are reserved to the copyright owner. The issue of what is a public performance is not defined in the legislation. It would seem clear, however, that the operation of a computer game programme within, for example, a public house or an amusement arcade, would constitute an infringing act if committed without the consent of the copyright owner.

8.15 Adaptation and Translation

Also significant in the list of infringing acts is that of making an adaptation of a protected work. In respect of a computer programme it is provided that this includes the making of 'an arrangement or altered version of the programme or a translation of it'. Translation is defined as including the making of a version of the programme in which it is converted into or out of a computer language or code or into a different computer language or code. The significance of this activity will be restricted to the situation where there is some form of access to the original programme source code.

8.16 Moral Rights

In describing the general features of the law relating to copyright, reference must finally be made to the concept of moral rights introduced into UK law under the 1988 Act. These rights have long been a feature of continental laws and, having been incorporated into the latest revision of the Berne Convention, were required to be introduced into the UK's system to ensure continued recognition of UK copyrights. The effect of the introduction of these moral rights is to extend a measure of legal protection to concepts of artistic integrity in addition to that which has traditionally extended to the more economic aspects of the work.

The moral rights are three in number. Fist, an author has the right to be identified as such in every copy of the work which is issued to the public. The significance of this right is Limited in the computer context. It does not extend to the author of a computer programme and, even in the situation where a handbook or instructional manual is prepared, the right does not extend to work which is carried out in the course of employment.

The second right is the converse of the above, referring to a false attribution of the work. In the literary field a statement on a book's cover to the effect that 'Conan Doyle's Famous Detective Returns' might in the absence of any other indication of authorship be taken as implying that the author was the famous Sir Arthur Conan Doyle. This right extends to aII works including computer programmes and to work carried out in the course of employment.

Finally, an author has the right to object to any derogatory treatment of his or her work. This right extends in respect of any 'addition to, deletion from or alteration to or adaptation of the work which amounts to distortion or mutilation of the work or is otherwise prejudicial to the honour or reputation of the author or director'.

Given the novelty of the section, no case Iaw exists concerning the conduct which Might be regarded as derogatory. Once again, however, the right will not extend to computer programmes and, in the case of a work created in the course of employment, will apply only if the author has been identified at the time of publication.

8.17 Resale and rental of copies of a protected work

In most cases a person who has lawfully come into possession of a copy of a protected work will have the right either to resell the copy or to make it available to members of the public on a rental basis. The Act provides an exception to this rule in the case of the rental of computer programmes, sound recordings and films. Essentially, such works may be hired only under the terms either of an order made by the Secretary of State or according to the provisions of a licensing scheme devised by the copyright owners and approved by the Copyright Tribunal.

Either procedure will prescribe terms upon which the rental may occur and the royalty that will be payable t the copyright owner. The justification for this provision Iies with the ease with which copies of software may be made. To this extent, the provisions for royalty

payments can be seen as offering some compensation for Iosses which may result from such activities.

8.18 Computer programmes as audio or visual works

A sound recording is defined in the legislation as:

> . . . a recording of sounds from which the sounds may be reproduced . . . regardless of the medium on which the recording is made or the method by which the sounds are produced or reproduced.

In many instances the digitized squawks and screams emanating from a computer game will not satisfy any criterion of originality for the grant of copyright protection. There would appear no reason to doubt that where the audio content is more sophisticated, this will not benefit from protection in its own right.

8.19 Digital Sampling

The practice of digital sampling is commonplace in the musical industry. With the introduction of digital technology it has become possible to represent any sound as a unique digital code. In this respect a compact disc is not unlike a computer programme whose contents are decoded by the associated player. For the Listener, the change from the previous, analogue, method of recording is claimed to lie in a more accurate production coupled with greater durability in the recording medium.

For those involved in the production processes other forms of activity become possible. Any information that can be recorded in digital format can be processed. This might be utilized to eliminate defects or extraneous sounds in a recording. The process of digital sampling is another and controversial application. As the name would suggest, digital sampling involves recording a small portion of an existing work: This will encompass not only the musical element but will also capture the particular style of the musician involved.

The ability to process digital information means that this material may be modified or may be merged imperceptibly with other materials to produce a new work. The copyright implications of this new practice raise few issues of principle but many extensive practical

problems. There can be no doubt that the making of a recording of a protected musical work will constitute an infringement of copyright. The practical problem will be to establish whether the portion copied represents a substantial portion of the work. Although the criterion is qualitative rather than quantitative, reproduction of a few bars of music may not suffice. A further issue may arise when the sampled work is modified.

Treatment will be regarded as derogatory if it amounts to 'distortion or mutilation of the work or is otherwise prejudicial to the honour or reputation of the author'. It Will, of course, be a question of fact whether this is the case.

8.20 Computer Programmes as Photographs or Films

The question whether the screen displays produced by a computer programme might be protected as photographs or films in their own right is one which is of potential significance. Disregarding the issue of whether reproduction of the appearance of a computer programme might constitute infringement of copyright in the controlling programme, reproduction of the appearance would, of itself, constitute an infringing act. In the Copyright Act 1988 a photograph, which is protected as an artistic work, is defined as:

> . . . a recording of light other radiation on any medium on which an image is produced or from which an image may by any means be produced, and which is not part of a film.

This provision will effectively be limited to the situation where a single screen display (or a number of discrete displays) are produced by a computer programme. With the advent of digital cameras it is quite possible for images to be recorded directly onto a computer disk and viewed on a computer monitor. The difficulty with the 1988 definition will concern the question of whether the working of such cameras involves the making of 'a recording of light or other radiation'. The definition of a film appears more relevant. The 1988. Act refers to 'a recording on any medium from which a moving image may by any means be produced'. This definition is wider than that which applied under the 1956 Act and which made reference to:

Any sequence of visual images recorded on material of any description (whether translucent or not) so as to be capable, by the use of that material, either of being shown as a moving picture, or of being recorded on other material whether translucent or not) by the use of which it can be so shown.

The adoption of an amended definition was intended to eliminate any doubt as to whether a copy of a film on video tape would be protected. The form of words used in the 1988 Act appears wide enough to cover the storage of moving images on a computer disk or tape. The availability of this form of visual copyright would be highly attractive to the owners of copyright in many computer programmes. As will be extensively discussed in the following chapters, there remains doubt how far the provisions of literary copyright will confer protection in the event that a second programme. replicates aspects of the functioning and appearance of an earlier work but does so using a different form of code.

The point was made by Sir Robert Megarry VC in one of the early interlocutory cases involving copyright in programmes that:

If I may take an absurdly simple example, 2 and 2 make 4. But so does 2 times 2, or 6 minus 2, or 2 per cent of 200, or 6 squared divided by nine, or many other things. Many different processes may produce the same answer and vet remain different processes that have not been copied one from another.

Protecting the result achieved by a computer programme rather than (or in addition to) the manner in which it is produced offers a potentially significant extension in protection. A number of arguments can be advanced against the application of provisions relating to copyright in films. With a film, a variety of forms of copyright will apply. The work may be adapted from a book or books which will be protected in their own right. It is very likely that there will be some written script which will again be protected.

The soundtrack accompanying the film will be protected as a sound recording. Finally the film will be protected in its own right. The film is, however, more than the sum of the other protected parts. It represents the product of the Director's skill and labour together with that of the other persons involved in its production.

The visual appearance of a computer programme, by way of contrast, is the product of nothing more than the operation of the programme. To protect it as a film would be to confer double protection upon the same subject matter. A further argument against the classification of a computer game as a film will lie in the fact that the user will play an active role rather than the passive one associated with the viewer of a film.

The options that the user may exercise, however, will be circumscribed by the format of the programmes. To this extent the user is merely exercising options presented by the producer and is not independently creating a new composite work. Arguing in favour of the extension of protection it is the ca se that there is nothing in the legislation to state that computer programmes are to be protected only as literary works. Some programmes, especially those in the entertainment sector; would appear more akin to films or other artistic works than any literary compilation. Even assuming that this form of protection might be available, the question will remain how useful it might be. It is an infringement of copyright in a film to take a photograph of a substantial part of its constituent images)

A competitor who photographed various screen displays to use as an aid in replicating their appearance will be in infringement of copyright. Although the point is not settled, it would appear that the act of reproducing a protected film must involve reproduction of the images themselves. A subsequent producer who utilized the same camera positions and techniques and re-created the sequence of events would not infringe copyright on this basis (although there might be infringement of some of the other forms of copyright subsisting in the original work). On this analysis, the scope of the protection is limited to, the act of direct reproduction of the work.

The independent production of even the identical images would not constitute infringement. Beyond the situation where an image is produced through the operation of what is clearly a computer programme lie developments in the field of interactive video. Such products, which are increasingly being used in the educational sector, enable a large number of film images to be processed in accordance with input from a user to produce a continuous display.

To sum up it may be said that there are several dimensions of copyright violation is the Digital era of internet and software. However drawing upon the historical precedents substantial legal remedies are evolved for this purpose.

In the United State for protection of copyright (software, movie sound tracking) piracy one can approach the FBI local office if imported. U.S. custom service local office for legal enforcement.

In India the Copyright Act provides protection right against any scientific or literary work. For the enforcement of violation of copyright the owner can approach the local police

authority for protection of right; however, the filing of First Information Report (FIR) by the police authority after taking time and it helps the pirator to destroy the evidences. In this connection the IT Bill provides adequate power to Deputy Superintendent of Police or Officer above him to act immediately to catch hold the pirator with evidence.

8.21 IPR in Software: An Indian Perspective

Did you know that any original published or unpublished literary work automatically becomes Copyright and is protected by simply recording it in any tangible form? Did you know that India has some of the most stringent Copyright laws in the world? Did you know that under the Copyright Laws, the term 'Literary Work' includes computer programmes; tables and compilations including computer databases?

This article aims to throw light on issues regarding Intellectual Property Rights and legal safeguards that are available to protect these rights.

8.22 How to be copyright protected

Any original published or unpublished literary work automatically acquires Copyright and is protected by simply recording it in any tangible form. All one needs to do is document or record the work on some tangible medium like ROM, magnetic tape, diskette or paper to get Copyright protection. This means that one does not necessarily have to go through the process of registering with the Copyright Office to get Copyright Protection, although it is advisable to register programmes with the authorities.

What does copyright protection actually mean?

Copyright provides the owner of an original work sweeping rights to do as he wants with his work. Copyright also confers a number of rights, some or all of which can be granted to others either exclusively or non-exclusively by the owner. He can reproduce his work in any material form including the storing of it in any medium by electronic means. He can release copies of the work to the public if they are not already available. He can translate or make any adaptation of the work. The owner can sell or hire out, or offer for sale or hire a copy even if such a copy has been sold or given on hire on earlier occasions.

What constitutes infringement of copyright?

Significantly, an infringement need not necessarily be an exact or verbatim copy of the original but its resemblance with the original in a considerable measure is sufficient to indicate that it is a copy The law will consider Copyright infringed if any one without permission from the owner of the Copyright or the Registrar of Copyrights does anything that is against rights of the owner. Additionally, the work cannot be created for sale or hired or distributed for trade of for any purpose that will affect the rights of the owner by any one.

The law is very clear about the parameters that bind a licensee as well. A computer programme licensee does not have the right to lend or otherwise transfer programme copy, unless authorized by the Copyright owner.

8.23 Legal action

The powers endowed on the Copyright law enforcement authorities are designed to ensure speedy action and redressal. Under the law, any Police Officer, not below the rank of Sub Inspector, may, if he suspects that a Copyright offence is being perpetrated, seize without warrant, all copies of the work, and all plates used for the purpose of making copies, wherever found. He should produce them before a Magistrate as soon as possible.

In the eventuality of an infringement being reported, the Courts are empowered to grant the following relief:

- temporary and permanent injunctions;
- impounding and destruction of all infringing copies, including master copies;
- actual monetary damages plus the infringer's profits ·statutory damages;
- court costs and reasonable attorney's fees.

Offenders, in the past, almost always used the slow pace of the judicial system to good effect. But the authorities have started using an effective weapon to deal with this problem with the Anton Piller action order. Anton Piller order allows a Local Commissioner, appointed by the court and sometimes accompanied by the Copyright owners' representatives, to enter the premises of the suspected counterfeiter and assist in identifying the infringing goods. An Anton Piller order can authorize the Commissioner to seek police assistance, break locks or set up decoy purchases. The Commissioner is the "eyes and ears" of the court, so to speak. This has dramatically: improved results as the infringers quickly come forward to settle the

case with the Copyright owner. These civil orders provide quick relief to the petitioner and provide an additional enforcement avenue to protect Intellectual Property Rights.

A good example of the potency of Anton Piller order is the recent action by the National Association of Software and Services Companies (NASSCOM) in conjunction with the Business Software Alliance (BSA) against two well known Computer Training Centres in New Delhi. These were the first set of anti piracy actions against an end user by NASSCOM and BSA. An important feature was that the case was settled in a record span of 10 weeks. The settlement included the payment of damages to the BSA and an agreement to legalize all software used at the centres. The infringers also provided an undertaking that they would not in future use, copy, sell, offer for sale or deal in any NASSCCJM and BSA member software illegally.

The laws are there, the enforcement authorities are vested with enough powers to protect Copyright. The concern is the lack of awareness among citizens. Every time a consumer buys a computer loaded with unlicensed software, or buys unlicensed software products he is party to this crime. The menace of software piracy or violation of Copyrights affects not only the potential of software development in India but also our country's economy, besides sending negative signals to potential investors.

Case 1

CONNECTIX SCORES PARTIAL LEGAL VICTORY AGAINST SONY

Connectix won a partial victory today in its legal battle against Sony Computer Entertainment over the Virtual Game Station, a software programme that lets consumers run PlayStation games to on a personal computer.

A federal court judge in San Francisco threw out seven of nine counts in a suit brought by Sony that alleged Connectix violated the entertainment giant's copyrights. Judge Charles Ledge also said he would decide in the next 90 days whether to review the remaining trade secret and unfair competition claims in the suit.

Sony has also filed a separate suit alleging patent infringement, and a Sony representative said the company intends to pursue the remaining complaints.
"We're obviously moving forward with those," said Sony spokeswoman Molly Smith.

An appeals court in February threw out a temporary injunction that Sony had received on the copyright claim that would have prevented Connectix from distributing its software. Connectix said it is also moving to dismiss the patent infringement claims.

"We are confident that we will prevail on the remaining issues," said Connectix chief executive Roy McDonald in a statement. "We hope that this decisive outcome will allow both parties to quickly close this matter and find ways to mutually benefit from our innovative cross platform technology."

The San Mateo, Calif.-based firm released its Virtual Game Player in January but was hit almost immediately with legal action from Sony. The programme allows games for the original PlayStation console to be played on a Macintosh or Windows-based computer.

A hearing in Sony's patent case is set for May 19 , Connectix said. Related 1550993 1548452 341586

Source.: Ian Fried, "Connectix Scores Partial Legal Victory against Sony', (NET News.com., May 16, 2000.

8.24 Short Summary

- Copying must involve a degree of intention on copyist.
- The issue of unconscious copying has also risen in a number of cases concerned with musical works.
- Concept of Fair dealing permit a degree of copying of a protected work.
- The act of performing the protected work in public are reserved to the copyright.

8.25 Brain Storm

- Discuss about the right of copyright owner.
- Define Literal and non-literal copying.
- Describe Error Correction.
- Explain Briefly about IEP in software.
- Give note an Legal action.

Lecture 9

Surveillance Through Information Technology

Objectives

In this Lecture you will be able to

- Know about privacy and Surveillance
- Describe about the Legal Response to data Surveillance

Coverage Plan

Lecture 9

9.1 Snap Shot – Introduction

9.2 Privacy and Surveillance

9.3 Forms of Surveillance

9.4 The Impact of Technology

9.5 Surveillance in the 1990s

9.6 Consequences of data Surveillance

9.7 The Legal response to data Surveillance

9.8 Short Summary

9.9 Brain Storm

9.1 Snap Shot - Introduction

The classic definition of the privacy concept is that it consists of the 'right to be left alone'. In terms of isolation from the scrutiny of others, the average individual living in a town or city enjoys vastly more personal privacy than did our ancestors living in small villages where every action was known to and a source of comment for neighbours. In some senses, it may be suggested that there is too much privacy in modern society; that excessive interest in the lives of our neighbours has been replaced by excessive in difference. As Steven Rodata has commented, privacy can be regarded as an 'elitist concept' and that:

> ... the right to be let alone can acquire a heavily negative meaning when this implies a disregard for the conditions of the less wealthy, abandoning the weakest to social violence.

The right to privacy receives a measure of recognition in the European Convention on Human Rights which provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence'. To an extent greater than with other basic human rights, the right to privacy must be subject to considerable qualification and, as epitomized in the ongoing debate concerning the allegedly intrusive nature of media activities, the right to privacy has to be balanced against a basket of other rights. Those identified in the European Convention include the right of free speech and the right to acquire information.

Although the intent to incorporate the terms of the European Convention into domestic law has been announced by the government, it is clear that no general right to privacy exists at present under English law. In the case of Malone ii Metropolitan Police Commissioner (No 2),. Megarry VC rejected a, contention that the tapping of Malone's telephone in the course of a criminal investigation violated his right to privacy:

Holding that there was no authority to support such a proposition, he stated, 'It is no function of the court to legislate in a new field. The extension of existing laws and principles is one thing; the creation of an altogether new right is another'. In 1990, the Court of Appeal was faced with a similar line of argument in the case of Kaye v Robertson. Kaye, a well-known actor, had suffered severe head injuries and had been hospitalized.

A reporter and a photographer secured access to his hospital room and took photographs of the injured person. It was intended that these should form the basis of a feature in a Sunday newspaper. An action was brought on behalf of Kaye, seeking to prevent publication of the material. An injunction to this effect being granted in the High Court, the defendants appealed. Holding that an arguable case had been made that the tort of malicious falsehood had been committed, the Court of Appeal continued the injunction in modified terms. All of the judges, however, were critical of the absence of a right to privacy, Bingham LJ commenting that:

> If ever a person has a right to be let alone by strangers with no public interest to pursue, it must surely be when he lies in hospital recovering from brain surgery, and in no more than partial command of his faculties. It is this invasion of privacy which underlies the plaintiff's complaint. Yet it alone, however, gross, does not entitle him to relief in English law.

9.2 Privacy and Surveillance

One of the key distinctions drawn in discussions of the right to privacy is between an individual's private and public personae. In countries such as the United States where a right to privacy is recognized, the right effectively ceases when an individual moves outside private property In such circumstances, the act of watching an individual's movements tends to be considered under the title 'surveillance'. In the past, surveillance has been considered something which is primarily carried out by or on behalf of society as a whole (government).

Although the act of placing an individual under surveillance may of itself modify individuals' behaviour patterns, in general surveillance is a means to an end which may significantly affect other interests of the data subject. An obvious example might be the surveillance of an individual suspected of involvement in criminal activity. The act of surveillance may lead to arrest, interrogation, trial and imprisonment. Much of the debate concerning the establishment of a right to privacy had centred on activities carried out by organizations and individuals with the private sector.

In the 1970s the remit of the Committee on Privacy was restricted to the private sector-albeit contrary to its wishes. One of the recurring themes in the field of information technology and the Law is that of convergence. The application of information technology is serving to blur traditional distinctions between activities, technologies and regulatory schema. This

phenomenon is apparent in respect of the present topic where increasingly surveillance is conducted within the private as well as the public sector. Dame Stella Rimington, former head of Ml5 has pointed out that concerns about the surveillance activities of security agencies should extend also to private sector operations:

> Although Big Brother was listening, he was doing so only for the purpose of defending our safety and well-being and there was a complex system in place to stop him doing more than was proportionate and justified.
>
> But there are some other Big Brothers in today's society over whom there are practically no controls. . . . Admittedly they do not tap your telephone or bug your house-at least I don't think they dc-but they certainly intrude into your privacy Have you thought that every time you use your loyalty card at Tesco or Safeway a computer logs up your name and address, where you shopped and on what day; what kind of based beans and whether you smoke or drink gin.
>
> All this information is logged away and cross-related and used in ways over which you have no control. If you use your bank card in cash dispenser machines or to pay bills you leave a trail behind you as you move around the country

The notion of a single all powerful computer is no longer relevant but the ease with which data may be transferred from one computer network to another; a phenomenon epitomized in the Internet, is serving to break down boundaries between systems. Techniques such as data mining strive to extract the last ounce of value from raw data whilst the practice of data matching enables linkages to be made between the contents of what were previously discrete data banks. Once again, the notion of convergence becomes apparent. It is not only significant in respect of linkage between different systems but also serves to break down traditional boundaries between public and private sector applications. It has been reported that Greater Manchester Police make use of credit reference agencies in order to identify the addresses of individuals. This source, it is claimed, is more current and detailed than the Police National Computer. Information held by credit reference agencies has also been accessed by insurance companies in determining whether to accept applications for motor vehicle insurance. Again, much of the administration of the tax system has been contracted out to private sector organizations.

9.3 Forms of Surveillance

In 1971 Alan Westin, in his seminal work Information Technology in a Democracy, identified three forms of surveillance; physical, psychological and data through digital satellite transfer At that time clear distinctions could be drawn between the three categories. Physical

surveillance, as the name suggests, involves that act of watching or listening to the actions of an individual.

Such surveillance, even making use of technology, has tended to be an expensive undertaking capable of being applied to a limited number of individuals. It has been estimated, for example, that a team of eight people would be required to place an individual under discreet surveillance on a 24-hour basis: Examples of psychological surveillance include forms of interrogation or the use of personality tests as favored by some employers. Once again, logistical and cost constraints have served to limit the use of these techniques. The end product of any form of surveillance is data or information. With both physical and psychological, surveillance, an active role is played by the watcher. Data surveillance involves a different, more passive, approach. Every action of an individual reveals something about the person. Very few actions do not involve individuals in giving out a measure of information about themselves. This may occur directly, for example in filling out a form, or indirectly, as when goods or services are purchased. The essence of data surveillance lies in the collection and retention of these items of information.

The possible effects are identified in a frequently quoted passage by Alexander Solzhenitsyn:

> As every man goes through life he fills in a number of forms for the records, each containing a number of questions . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If all these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would lose the ability to move . . . They are not visible, they are not material, but every man is aware of their existence . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

Beyond the acquisition of information as an end in itself, the portability of computerized data has the potential to break down the invisible walls which serve to divide our lives into a number of discrete compartments. The potential dangers were described by Browne-Wilkinson VC in Marcel v Metropolitan . Police Commissioner. Documents belonging to the plaintiff had been seized by the police in the course of a criminal investigation.

Civil proceedings were also current in respect of the same incidents and a subpoena was served on behalf of one of the parties to this litigation seeking disclosure of some of these documents. Holding that the subpoena should be set aside, the judge expressed concern that:

> . . . if the information obtained by the police, the Inland Revenue, the social security offices, the health service and other agencies were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state.

Although this ruling was overturned in the Court of Appeal, g , Nolan LJ expressed agreement with the proposition that strict limits must be placed upon the se to which the seized documents can properly be put by the police'.

9.4 The impact of Technology

Technology, like love, changes everything. With the ability to digitize any form of information, boundaries between the various forms of surveillance are disappearing with the application of information technology linking surveillance techniques into a near seamless web of surveillance. Developments in data processing suggest that the distinction between informational and physical privacy is becoming more and more flimsy.

The reach of systems of physical surveillance has been increased enormously by the involvement of the computer to digitize and process the information received. Car number plates are scanned by police television cameras and the details transmitted for immediate checking by computer against lists of stolen or 'wanted' vehicles. As the network expands it is suggested that:

> . . . it could become possible to find or follow almost any vehicle in Britain simply by tapping its registration number into a computer keyboard.

9.5 Surveillance in the 1990s

Increasing numbers of closed circuit televisions monitor movement W the streets whilst countless thousands of cameras are operated by commercial operators to monitor our movements in shops and offices and car parks. 'Intelligent' cameras allow images of individuals to be compared with a database of suspected persons.

Twenty faces can be scanned per second and the results compared with a data base of one million images. Surveillance devices in the workplace allow employers to monitor the

activities and efficiency of individuals. Most word processing packages maintain records of the time spent working on particular documents. Even the Internet and WWW which are often touted as the last refuge of individualism might equally accurately be described as a surveillance system par excellence. An individual browsing the Web leaves electronic trails wherever he or she passes.

A software programme known as a 'cookie' may be transmitted from a Web site to the user's computer and remain there until the site is next accessed at which time details of the user and previous visits to the site will automatically be transmitted. Many users may participate in Internet newsgroup discussions. Although messages will disappear from most sites after a few days, systems such as DejaNews archive copies of all postings and provide the facility for users to search postings by reference to criteria including the name of the poster.

It is, therefore, a comparatively simple matter to obtain a complete list of all messages written by a particular individual. This information might have attractions for direct marketers, prospective employers and even, given the nature and content of some newsgroups, potential blackmailers. Virtually any object may now be represented in digital format. Music, pictures, text, sound are all the subject of digitization. Even three-dimensional objects may be transformed in .this manner. One of the more ghoulish sites on the Internet contains the digital record of the body of an executed person. The physical body was sliced into 1,870 sections, these were photographed, the images digitized and re-assembled in a computer. Now, it is reported:

> Surgical students will perform autopsies and operations on the Visible Man who will eventually have elasticity in his tissues and 'bleed' and react as a 'living' human. Doctors will be able to introduce cancer and learn how best to fight the illness. Scientists will introduce aging and see exactly why and how it occurs.

It is reported that the Visible Man is to be joined in Cyberspace by a Visible Woman, Boy, Girl and Baby. When talking of personal data, it is difficult to identify anything more personal than this, although the death of the subjects will ensure that no legal rights, whether to privacy or otherwise, are infringed.

Developments in the technology of virtual reality may have similar results but involve living individuals. The possibility that aspects of an individual's personality and appearance might be captured for the purpose of 'virtual sex' has formed the focus of at least one novel and

been considered at a more academic level in a number of publications dealing with the technology.

Surveillance through satellite cameras is increasing tremendously. The National remote sensing technologies of each space power countries are scanning the important data and digitizing the information for various purposes such as crime prevention, scientific application, forecasting etc.

9.6 Consequences of Data Surveillance

As far back as 1972, in considering the threats to privacy resulting from computerized data processing, the Younger Committee identified the prospect that:

Because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the records or what is happening to them.

In the report; this prospect was put forward as a cause of public concern. Much subsequent evidence would dispute this. Hundreds of thousands of individuals have applied for supermarket 'loyalty cards'. Such cards provide an invaluable point of linkage between details of individual transactions and the more generic stock management computer systems which have long been a feature of retail life.

The seller now knows not only what has been bought but also who has bought it, when, in conjunction with what other products, and what form of payment has been tendered: Analysis of the information will reveal much about the individual's habits and life style which may be used as the basis for direct marketing targeted at the individual customer. It is, of course, difficult to identify the specter of totalitarianism behind a supermarket loyalty card.

Many of the recorded instances of the misuse of information have occurred not as part of the original design but as a by-product of the fact that the information is available. The story has been told how the elaborate population registers maintained by the Dutch authorities prior to the Second World War (no doubt with the best possible motives) were used by the invading Germans to facilitate the deportation of thousands of people.

In this case, as in any similar case, it is clear that it was not information per se that harmed individuals, rather it was the use that was made of it. In this sense information is a tool; but a very flexible tool, and whenever personal information is stored the subject is to some extent 'a hostage to fortune'. Information which is freely supplied today, and which reflects no discredit in the existing social climate, may be looked upon very differently should circumstances change. it may, of course, be questioned how far any legal safeguards may be effective in the event of an external invasion or unconstitutional usurpation of power. In discussion of this point in Sweden it has been suggested that:

Under a threat of occupation there may be reason to remove or destroy computer installations and various registers in order to prevent the installations or important information from falling into enemy hands. An enemy may, for example, wish to acquire population registers and other records which can assist his war effort. There may be reason to revise the plans as to which data processing systems should be destroyed or removed in a war situation.

Whilst such plans and procedures might appear to afford protection against the possibility of outside intervention it must be recognized that, in the past, the use of personal information as a weapon against individuals has not been the exclusive province of totalitarian states. Again during the Second World War, the United States government used information supposedly supplied in confidence during the census to track down and intern citizens of Japanese ancestry

More recently it has been reported that the United States Selective Service system purchased a list of 167,000 names of boys who had responded to a promotion organized by a chain of ice cream parlors offering a free ice cream on the occasion of their eighteenth birthday. This list of names, addresses and dates of birth was used in order to track down those who had failed to register for military service.

Such practices illustrate, first, the ubiquitous nature of personal information and, second, that no clear dividing line can be drawn between public-sector and private-sector users as information obtained within one sector may well be transferred to the other. At a slightly less serious level, it was reported in the United Kingdom that information supplied in the course of the 1971 census describing the previous occupations of respondents was passed on to health authorities who used it to contact retired nurses with a view to discovering why they left the profession and to encourage them to consider returning to work.

Whilst it may be argued that no harm was caused to the individuals concerned by the use to which this information , was put, it provides further evidence of the ubiquitous nature of information and of the ease with which information supplied for one purpose can be put to another use. Information technology is an enormously powerful tool. It has the capability to record vast amounts of data which might previously have been held only in some human memory, to process it in ways which would previously have been impracticable, to transmit and share information with other information technology systems and networks on a world-wide basis and to retain the information for a potentially unlimited period of time.

The notion of the black sheep of a family leaving debt and scandal behind to seek fame and fortune in a far flung country may well have been consigned to the history books. 'The Christian notion of Redemption' it has been suggested, 'is unknown to the computer'. Today's vast data banks contain the raw material for misuse and oppression on a scale previously not imagined.

The benefits of information technology are, of course, immense and many facets of modern life are totally dependent upon the technology. Whilst dangers can never be eliminated; there is need for informed public debate as to options and choices. Proper regulation is in the interests of the technophile as much as the technophone.

9.7 The Legal response to Data Surveillance

We live in uncertain, challenging and interesting times. Few aspects of life will survive the information revolution. unscathed but this is itself a natural process. Any attempt to apply yesterday's concepts to tomorrow's society is. futile. Privacy both as a legal and a philosophical concept has a nebulous and at times contradictory meaning: In essence, it cannot exist in isolation but must always be balanced against other interests and claims. To attempt to rely upon it as the basis for a schema to regulate information technology is surely doomed to failure, especially in the United Kingdom where there is no tradition of a legally enforceable right to privacy All too often, it would appear, we are willing to sell our electronic souls for a can of beans.

Personal privacy may be in danger of disappearing amidst public indifference and perhaps even acclaim. If a major element of privacy is the right to be free from unwanted surveillance, in the situation where individuals freely give out information about themselves, there clearly is no sense of invasion of privacy. We can no more make a person feel that his or her privacy has been breached than we can make that person appreciate a Beethoven symphony or an Oasis concert.

Virtually every relevant survey of public opinion, however, indicates that personal privacy is highly valued as a concept. A partial answer to the conundrum may lie in the difficulty of defining privacy. Clearly many (perhaps most) of the population do not regard information gathering activities of this nature as a significant impact upon privacy. As soon as we move from the most abstract definition all too often we fail to recognize what it is or, more significantly; what might constitute its infringement or violation. On occasion, plans to engage in certain forms of data processing have created a climate of public opposition sufficient to cause their withdrawal. Australia, plans to introduce a system of universal personal. Identifiers were withdrawn following public opposition. In the United States, plans by the software company Lotus to sell a directory of all citizens, 'Market Place', were dropped. following a similar public outcry. At a less intense level, a debate is being conducted in the UK as to the merits of introducing a national system of identity cards where each card would contain information about the subject in electronic format.

In India also with growing international awareness of such things; issues concerning census data, PAN data residing with IT Authorities, votes card etc. are becoming a matter of public debate and censure.

9.8 Short Summary

- The classic definition of the privacy concept is that it consists of the 'right to be left alone".
- One of the key distinctions drawn in discussions of the right to privacy is between an individual's private and public personal.
- Developments in data processing suggest that the distinction between international and physical privacy is becoming more and more flimsy.
- Surveillance devices in the workplace alone employers to monitor the activities and efficiency of individuals.

9.9 Brain Storm

- What is meant by privacy and Surveillance?
- What are the consequences of data Surveillance?
- What is the legal response to data Surveillance?

Lecture 10

Individual Rights and Remedies

Objectives

In this Lecture you will be able to

- Know about Implementing Subject access
- Know about Law enforcement and taxation

Coverage Plan

Lecture 10

10.1 Snap Shot - Introduction

The concept of subject access is undoubtedly the feature of data protection legislation which has the most direct impact upon data subjects. Its essence is contained in the seventh data protection principle which provides that:

An individual shall be entitled

a. at reasonable intervals and without undue delay or expense

   i. to be informed by any data user whether he holds personal data of which that individual is the subject; and
   ii. to access to any such data held by a data user; and

b. where appropriate, to have such data corrected or erased.

The directive also makes provision for subject access, article 12 providing that:

Member States shall guarantee every data subject the right to obtain from the controller:

a. without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as. to the purposes of the processing, the categories of' data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

b. as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
c. notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

In common with most of the data protection principles, this general statement requires considerable elaboration if it is to be applied in the context of particular processing activities. In this chapter, consideration will be first given to the manner in which access rights may be exercised before attention is paid to the inevitable exceptions from access and as to the remedies which may be available to an aggrieved individual whether for breach of the subject access provisions or of other elements of the legislation.

10.2 Implementing subject access

The essence of the right of access may be stated briefly. Any data subject may contact any data user or controller with the question whether the latter holds any personal data concerning the applicant. If the answer to this question is in the affirmative a copy of the information may be requested) under the act a user is required to supply a copy of the information held complete with an explanation of any terms which 'are not intelligible without explanation'.

The Directive's formulation is broader requiring that the data be 'communicated in an intelligible form . It would appear that this might encompass verbal delivery of the information or its inclusion in an e-mail, message. Additionally, the Directive requires that where decisions affecting the individual are made on the basis of automated processing, ; information must be supplied as to the logic involved in the processing.

Both Act and Directive provide that requests may be made at reasonable intervals and that a reasonable (not excessive) fee may be charged. In determining how frequently a subject may seek to exercise access rights the Act provides only that:

In determining whatever access to personal data is sought at reasonable intervals regard shall be had to the nature of the data, the purpose for which the data held and the frequency with which the data are altered.

The cost of access receives more precise treatment, it being provided that a fee of up to £ (pound sterling) 10 may required by a data user.' Although the value of the fee has be eroded by a decade of inflation, its amount was the source some surprise and concern at the time of its introduction Comparison may certainly be made with the situation exits in respect of requests for access to credit reference agency fi under the access provisions of the Consumer Credit Act, 19'. where the fee required is £ (pound sterling) 1. Although it m be argued that credit reference agencies' operations a designed to make it easy (and cheap) to extract all of t information about an individual,' a situation which may I be replicated in other areas of data processing, such a discrepancy is hard to justify. ,

Two further factors concerned with the operation of ! subject access principle may make the process more financially daunting. A data user is entitled to require payment of the prior to making any response to a request for access. Ten pounds may be required, therefore, in order for the enquiring data subject to be told that no personal data is held. Perhaps more significant is the consequence of the availability of multiple registrations or notifications. A user is entitled to require a fee in respect of each entry on the register to which a request for access refers. Given that a large user may have several thousand entries, the cost of access could become prohibitive. Even when, as will normally be the case, many entries will clearly not relate to persons such as the enquirer, the cost of access could easily amount to several hundred pounds. There would appear to be no requirement that these situations be altered in implementing the Directive.

10.3 Enforced subject access

In certain areas, notably where access is sought to data relating to criminal convictions, it appears that most requests are made at the instance of a third party, typically a potential employer. In other areas such as examination marks, employers are increasingly aware that individuals have rights of access to information and require that these rights be exercised with a copy of the information being supplied to the potential employer. Such conduct would seem contrary to the purpose of the access right as a means for empowering individuals, and

the Registrar in his 1989 review of the legislation proposed that enforced subject access should be prohibited.

In early drafts of the Directive it was stated explicitly that a data subject should be entitled to:

. . . refuse any demand by a third party that he should exercise his right of access in order to communicate the data in question to that third party or to another party unless the third party's request is founded on national or Community la.

The final text is less specific' although it appears that the phrase requiring access be obtained 'without constraint' is intended to secure the same result. The ambiguity lies in part in the English translation, with other texts, for example the German, making reference to access being 'frei ungehindert' while the French reference to access 'sans contrainte' is generally translated as meaning 'without duress'.

Although the Home Office Consultation paper was silent on the topic, the White Paper indicates an intent to 'put an end to the practice'. The manner in which this is to be done remains undecided an indeed it may be questioned how far it will be possible to terminate the practice? In the situation where an individual is seeking work, the mere suggestion from a potential-employer that a copy of information would be helpful can easily Assume the form of a command.

10.4 Access procedures

Having established the principle of access, the legislation prescribes the procedures under which the right may be exercised. Although no particular form of application is specified, a user is obliged to respond only to requests which are made in writing and which contain such information as may reasonably be required to confirm the identification of the data subject and allow location of relevant data. The question what information might reasonably be required by the data user is one which admits of no easy answer. Items such as customer or employee reference numbers might facilitate considerably the user's task but the difficulty will lie in determining whether a request for supplementary information is reasonable or whether it marks an attempt to dissuade the subject from pursuing the access request.

10.5 Providing access

A request for access must be met within 40 days from the date the request, or any supplementary information required is received. The information supplied to the user must generally be that which appeared on the computer at the time when the request for access was received. Such a provision is necessary to prevent a user from 'editing' a file prior to sending a copy to the data subject. It is provided, however, that where the information relating to the subject has routinely been amended between the date of receipt of the request and the date when a hard copy is made for transmission to the subject, the information applying at the latter date may be supplied.

10.6 Examination mark

The requirement to satisfy access requests within 40 days is subject to a partial exception in the case of examination results. Many examination authorities, especially those concerned with large-scale exams such as 'A' Levels, require more than 40 days to mark scripts. Preliminary marks, however, may often be entered on to their computers some considerable time before the formal publication of the results. This would open the door for candidates to seek to exercise their access rights under the Data Protection Act to obtain a preliminary indication of their results.

The workload incurred in responding to these requests might be such that the normal marking process' would suffer significant delays. The Act gives such bodies the option either of complying with the normal 40-day period or delaying a response for six months or, if earlier, 40 days after the publication of the exam results. This is not as generous a concession as might initially appear.

In the event the user delays a response, the information as ultimately supplied must include not only details of the final mark awarded but also any other information, perhaps in the form of provisional marks, which appeared on the computer at any time subsequent to receipt of the access request. Examination authorities may, therefore, have to maintain some form of audit trail permitting the recreation of the data held on their computers at a given point in time. In certain instances this provision might be used to prevent subject access.

Universities might routinely delete all examination records from their computers every 40 days. In this way the institution obtains the benefits of automated processing of the marks but ,ill always escape from the subject access provisions. Whilst it might be argued that this form of processing is unfair, and as such could constitute a breach of the first principle, it is also the case that the deletion of the data removes many of the dangers for individuals which prompted the introduction of data protection legislation. Obviously, the practice will be viable from the data user's standpoint only if they will have no further need for the data, at least in electronic format, after 40 days.

10.7 The extent of access

Data subjects are entitled to receive their own personal data. Obviously, they are not entitled to receive information about anyone else. The Act provides that a user shall not be obliged to comply with a request for access:

> ... if he cannot comply with the request without disclosing information relating to another individual who can be identified from that information unless he is satisfied that the other individual has consented to the disclosure of the information to the person making the request.

At first glance, this exception appears eminently reasonable as ensuring the third party's data protection. The operation of the principle may prove less happy.

Information identifying another individual includes anything which might identify that person as the source of data pertaining to the enquiring subject. Although the Act does go on to provide that the user shall be obliged to supply as much of the information relating to the subject as is possible without divulging the identity of the third party (the omission of names or other identifying particulars is specifically recommended) the result may be to put both subject and user in an invidious position. The major difficulty facing the data subject is that, although the Act provides for the possibility that the third party may consent to the disclosure of the data, this may occur only if a request is made to this end. Nothing in the Act obliges the user to seek this consent and the subject will, of course, not be in possession of the information to do so.

The position of a data user attempting conscientiously to comply with the requirements of the legislation may be no more enviable. Significant problems may arise in determining whether

and to what extent editing of the data might adequately conceal the third party's identity. Deletion of the name might suffice but much will depend on the nature of the information held by the data subject.

The user may have little knowledge of this. An example might be given of a situation where a report has been made to a local authority by a neighbour of the data subject alleging violent and anti-social behaviour. The information is held on computer and is subject to the provisions of the Data Protection Act. In the event that the subject seeks access, it might well be unwise, especially given the nature of the alleged activities, that the subject should be informed of the identity of the informant. The question arises, however, how much censorship of the data will suffice. If the subject should request access, it is difficult to know how the user should respond. If the subject lives in a city area, deleting the name of the complainant may be sufficient, although this may have the effect of causing the subject to nurture suspicions of a considerable number of persons. If the subject lives in a country area it is possible that only one of a very small number of people could have been the source and even an edited disclosure would reveal this fact. Again, the data user cannot be expected to be aware of any suspicions which the subject may have harboured concerning the possible identity of informants. Indication that a report has been received from an anonymous source might result in the subject blaming some totally 'innocent' party.

10.8 Data relating to children

One partial exception to the principle that only the subject is entitled to access under the seventh principle occurs where the data relates to a child. The extent to which an adult will be entitled to exercise subject access rights on behalf of a child is subject to the general law. For England and Wales, the Registrar has advised data users that they will be required to judge whether a child understands the nature of the access request. If this is the case, any response should be made to the child rather than a parent or guardian. The position may be simpler in Scotland. Under Scots law children are classed as either pupils or minors. Minority begins at 12 in the case of female and 14 for male children. Minors are considered capable of exercising access rights on their own account whilst this function will be carried out by a pupil's tutor.

10.9 Persons suffering mental disorder

Provision is made in the legislation for orders to be made regarding the exercise of access rights on behalf of a person suffering from a mental disorder. No action has been taken under this provision. Save in the situation where access might be refused on the ground that this would cause serious harm to the subject's health; there would seem no basis for refusing a request for access by a person suffering a mental disorder.

10.10 Exceptions to the right of access

In common with the approach adopted in relation to the non-disclosure principle, what the subject access principle gives with one hand, the body of the statute takes away with the other and a significant number of provisions restrict or exclude the right of access. In general there is no doubt that the Act's provisions in this respect will conform with the Directive which provides that:

Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

a. national security;
b. defence;
c. public security;
d. the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
e. an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters.
f. an monitoring, inspection or regulatory function connected, even occasionally with the exercise of official authority in cases referred to in (c), (d) and (e);
g. the protection of the data subject or of the rights and freedoms of others.

Given the limitation upon the Community's legislative competence discussed previously, it is doubtful whether restrictive measures relating to national and public security, defence, crime prevention and detection and taxation should come under the legislation in. any event. In these respects, the United Kingdom's provisions may also be compared with the obligations incurred under the Council of Europe Convention.

The headings under which the Act provides for access requests to be denied will require little change. One addition is likely in respect of expressions of intention. These may no longer be excluded from the definition of personal data but the Government has indicated the intent to exclude these from the subject access provisions. One caveat which might be raised concerning the approach of the United Kingdom legislation is whether the total exclusion from access sanctioned in the legislation will always comply with the Directive's (and indeed the Convention's) use of the adjective 'necessary' as providing the basis for restrictive measures.

In respect of medical data, for example, whilst the United Kingdom system provides for total exemption, albeit in limited circumstances, other regimes make special provision for the manner in which access is to be provided, perhaps following professional counseling. A similar approach applies in the United Kingdom in respect of adoption records.

Prior to considering the circumstances under which a user may legally deny a subject's access request, mention should be made of a problem that may arise whenever the user determines that all or part of a request for access falls within the scope of an exception. In such a case there is no requirement to inform the subject what has occurred. In the event that the user feels that all of the data held is covered by an exception, the reply may lawfully be made 'we do not hold any personal data concerning you'. Again, where elements of the data are suppressed in reliance on an exception, no indication of this need be given.

Under the Act's definitions, personal data is classed as data to which the subject is entitled to have access. Where an exception is properly relied upon it may be accepted that it is as undesirable from the user's standpoint to inform the subject that they hold data which they are not willing to disclose as it would be to divulge the information. In the event that a subject suspects that personal data has not been supplied pursuant to a request for access, action may be raised before the courts.

An alternative course of action will be to make a complaint to the Registrar. In the event the Registrar takes action, the onus will be on the user to justify their action. Dependent, however, upon the circumstances and the nature of the data, it may be that a subject who receives the reply that no relevant personal data is held may accept this at face value and will make no attempt to pursue the matter before the courts or with the Registrar.

10.11 Law enforcement and taxation

Where data is held for the purpose of

- the prevention or detection of crime,
- the apprehension or prosecution of offenders, or
- the collection or assessment of any tax or duty.

a request for access may be denied where this would prejudice the attainment of the purpose for which the data is held. The operation of this exception raises a number of significant issues. It is difficult to conceive of any item of personal data that could not be regarded as potentially relevant to the purpose of crime prevention.

The exemption will apply only where the grant of access would prejudice this purpose. In the event a denial of access is challenged before the Registrar, the onus will be on the data user to demonstrate a likelihood of prejudice in the circumstances of the particular case. Whilst these issues may be susceptible of ready resolution in the context of criminal detection and the apprehension or prosecution of offenders, some problems may be anticipated in relation to the nebulous concept of crime prevention.

To give an extreme and unlikely example, a police force may receive information that a person is planning to rob a bank. At this stage the information is held for crime prevention purposes. If the individual concerned should make a request for access it might be argued that the purpose of crime prevention would best be served by disclosing the information. Faced with this knowledge, it would be a foolhardy robber who continued with the particular scheme. It appears both unlikely and undesirable that potential criminals should receive such a helpful warning. It may be that the phrase 'crime prevention' could be interpreted in the sense of preventing the successful perpetration of the crime.

The holding of data or the purposes of crime prevention and detection or the apprehension arid prosecution of offenders is not limited to the police, other public law enforcement agencies. Proceedings raised by the Registrar against the Halifax Building Society involved the holding of personal he purpose of crime prevention.' These might, however, be expected to make up the bulk of the data users concerned with this provision and the effect of this provision will be to subject their record-keeping activities to an unprecedented degree of independent scrutiny.

10.12 Health data

Moving on from the areas of police and tax records, the Act provides for restrictions to the right of access in several other significant fields. Particular problems have been identified where medical records are involved. The convention recognizes that items of medical data possess an exceptional degree of sensitivity which may call for especially stringent controls to be impose upon those data users active in this field. It might appear to follow from this that the case for the operation of the subject access procedures is also exceptionally strong in this field.

The reality is, however, less clear-cut. Such records often include technical terms which are not, and may not realistically be rendered intelligible to a non-professional. Again, it may be argued that these records contain clinical assessments of a patient and a prognosis as to their future health prospects. Such data may frequently be provisional or speculative in nature and the grant of subject access may have the effect of causing unnecessary distress to the data subject. Taking the above factors into consideration the convention maintains a presumption in favour of access, providing that a request may be denied only where this is necessary in the interests of 'protecting the data subject or the rights and freedoms of others'. In seeking to give effect to the Conventions provisions. the Data Protection Act provides that the Secretary of State may:

. . . by order exempt from the subject access provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health of the data subject.

This power was exercised prior to the subject access provisions becoming operative with the making of the Data Protection (Subject Access Modification) (Health) Order, 1987. This applies in relation to data held or compiled by, or on behalf of, a health professional and establishes as the criterion for refusing an application for access the belief that this 'would be likely to cause serious harm to the physical or mental health of the data subject'.

In respect of all requests for access to data coming within the scope of the order, it provided that the decision to grant or to refuse the application must be made by the 'appropriate health professional'; defined as the medical or dental practitioner best qualified to advise on the patient's case or, in the absence of such a person:

. . . a health professional who has the necessary experience or qualifications to advise on the matters to which the information which is the subject of the request relates.

By providing that access may be denied only to the extent that this would cause 'serious harm' to the health of the data subject, the order must be seen as establishing a strong presumption in favour of access. Whilst recognizing that circumstances, particularly those connected with Psychiatric illness, may exist in which the supply of a copy of a medical record may not be in the best interests of the patient, it may be doubted whether the procedures adopted under the order are, in themselves, likely to prove any less harmful.

In common with the situations arising under other exemptions, a health professional may respond to a request for access with the statement that no relevant personal data is held. To an extent perhaps greater than with the other exceptions, the data subject is likely to be aware of the fact that data is held.

The failure to supply data may well be a source of distress in itself, whilst discovery of the fact that the data has been withheld for fear that access would cause serious harm to the patient's health would, in itself, appear inimical to his or her health interests. It may finally be noted in this context that the extent of the individual's right of access to medical records has been extended under the provisions of the Access to Health Records Act, 1990 to the situation where records are held in manual systems subject to equivalent exemptions to those contained in the Data protection Act.

10.13 Social work data

As is the case with medical records, the Data Protection Act adopts the view that, in certain situations, access to a social work record may be inimical to the data subject's interests. Once again, the legislation lays down general criteria and delegates regulatory power to provide for the detailed application of any exception. The Act here provides that the Secretary of State may modify or exclude the operation of the subject access provisions in respect of information:

a. held by government departments or local authorities or by voluntary organizations or other bodies designated by or under the order; and

b. appearing to him to be held for or acquired in the course of carrying out social work in relation to the data subject or other individuals;

Where it was considered that the operation of subject access might prejudice the carrying out of social work. Although this provision appears similar to that regulating the extent of access to health data, the empowering provisions differ in that, whilst in respect of health data the Secretary of State's discretion is unfettered; in the area of functions. Today, the provisions of the Data Protection (Subject Access Modification) (Social Work) Order, 1981 define the extent of subject access to social work data. Data will be regarded as held for this purpose if it is maintained in the course of specified statutory or voluntary functions. Thus it is provided, for example, that data maintained by the NSPCC will assuming it relates to a welfare function, be regarded as coming within the scope of the exemption. In these circumstances, access may be denied where it would be likely to prejudice the carrying out of social work by reason of the fact that

a. serious harm to the physical or mental health or emotional condition of the data subject would be likely to be caused; or

b. the identity of another individual (who has not consented to the disclosure of the information) either as a person to whom the information or part of it relates or as the source of the information would be likely to be disclosed to or deduced by the data subject or any other person who is likely to obtain access to it either from the information itself or from a combination of that information and any other information which the data subject or such other person has or is likely to have.

As is the case with health data, it is provided that this latter provision cannot be utilized in order to conceal the identity of the person responsible for the compilation o the record or a part thereof. Again, where data would lead to the identification of a third party, where possible, these details must be severed from the remainder of the record.

10.14 Judicial appointments

In England the Lord Chancellor's Office maintains a computerized data base containing information on those members of the legal profession who might be candidates for appointment to judicial office. Such data subjects will not be permitted access to the information, the Act providing that: Personal data held by a government department are

exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as information relevant to the making of judicial appointments.

This exemption is wider than that applicable under the general restriction of access to information supplied by a third party: here access will be denied even if the third party is willing for access to be granted or if the information could he censored so as to conceal the identity of the source. There must be doubt as to whether such an exemption conforms with the provisions of the Convention, denial of access not being justifiable by reference to any of the relevant interests there specified.

10.15 Short Summary

- Any data subject may contact any data user or controller with the question whether the latter holds any personal data concerning the applicant.

- Data subjects are entitled to receive their own personal data.

- By order exempt from the subject access provisions or modify those provisions in relation to, personal data consisting of information as to the physical or mental Health of the data subject.

- A health professional who has the necessary experience or qualification to advice on the matters to which the information which is the subject of the request relates.

10.16 Brain Storm

- Discuss Enforced Subject Access?
- Give notes on Providing Access?
- Describe about the extend of access?
- Explain Law enforcement and taxation?
- Discuss about Health data and Social work data?

Lecture 11

Legal Privilege

Objectives

In this lecture you will learn the following

- Regulation of financial services
- Order of secretary of state
- Rectification of inaccurate data
- Subject access in perspective

Coverage Plan

Lecture 11

11.1 Snap Shot

11.2 Regulation of financial services

11.3 Credit reference agencies

11.4 Information otherwise available to the public

11.5 Order of secretary of state

11.6 Failure to provide access

11.7 Matters arising subsequent to access

11.8 Rectification of inaccurate data

11.9 Compensation for inaccuracy

11.10 Compensation for unauthorized disclosure

11.11 Complaints to the registrar

11.12 Subject access in perspective

11.13 Short Summary

11.14 Brain Storm

11.1 Snap Shot

Information divulged in the course of the lawyer-client relationship has always been afforded a high degree of privilege by the courts. This protection could be negated were another party, perhaps engaged in litigation with the client, to be allowed to exercise his or her access rights and obtain a copy of any information about himself or herself which may have been passed on to the solicitor by the client or been obtained on the client's behalf. The Act attempts to avoid such a result by providing that the access provisions are not to apply where:

> the data consist of information in respect of which a claim to legal professional privilege (or, in Scotland, to confidentiality as between client and legal professional adviser) could be maintained in legal proceedings.

The exemption under the Data Protection Act extends beyond the situation where legal proceedings are in train or even, it would appear, contemplated. In this eventuality the criterion adopted would appear to call for a degree of speculation, with the parties called upon to decide whether a claim to confidentiality would be upheld in the event that legal proceedings were to be instituted.

11.2 Regulation of Financial Services

Much criminal detection will be conducted by police forces, a variety of criminal or quasi-criminal functions are exercised by other regulatory authorities. Where investigations are in train it may be as undesirable to permit subject access as is the case with police data. Accordingly, the Data Protection Act provides that the Secretary of State may provide that the access provisions are not to apply in respect of statutory functions ,here these are designed to protect the public:

> . . . against financial loss due to dishonesty, incompetence or malpractice by persons concerned in the provision of . banking, insurance, investment or other financial services or in the management of companies or to the conduct of discharged or undischarged bankrupts.

The scope of this provision was extended by the Financial Services Act, 1986 to include the activities of recognized self-regulatory authorities concerned with the maintenance of standards within the financial sector. In applying this principle the Data Protection (Regulation of Financial Services etc.) (Subject Access Exemption) Order was made in 19871 and contains an exhaustive list of the functions and the agencies.. w hose activities are to be exempted from the subject access provisions.

11.3 Credit Reference Agencies

Many credit reference agencies now maintain their records on computer. As such they are subject to the provisions of the Data Protection Act. The right of subject access to records maintained by such agencies has existed since the enactment of the Consumer Credit Act of 1974.

The Data Protection Act provides that, in respect of subject access, the provisions of the 1974 Act will prevail. This offers the data subject the advantage of a lower fee. In other respects, the provisions of the Data Protection Act will prevail. A number of the decisions of the Data Protection Tribunal have concerned the activities of credit reference agencies. In the course of these, the Tribunal explicitly rejected the claim that jurisdiction over the operation of such bodies lay more properly with the Director General of Fair Trading as the person responsible for the supervision of credit reference agencies under the Consumer Credit Act.

11.4 Information otherwise available to the Public

The subject access provisions will not apply in the situation where the data user is statutorily obliged otherwise to make the information available for public inspection, whether free of charge or upon payment of a fee.' This would be the situation, for example, with the electoral roll or with a public company's statutory accounts or, indeed, with the Data Protection Register.

11.5 Order of Secretary of State

The Secretary of State is given power to exclude the operation of the subject access provisions where the disclosure of data is prohibited or restricted under any other statute and where he considers that the prohibition or restriction ought to prevail over the access provision in the interest of the data subject or of any other individual. It was suggested in Parliament that this provision could be coupled with the Official Secrets Act of 1911 thereby enabling the Secretary of State to exclude any form of subject access to government-held information. Assurances were forthcoming that this was not the intention behind the provision and that the presence of the phrase 'in the interest of the data subject or of any other individual' meant : that the power could not be invoked in the interest of the government.

The regulatory power conferred in the Act was exercise of with the making of the Data Protection (Miscellaneous Subject Access Exemptions) Order, 1987. It provides exemption in respect of adoption records, certain educational records any information provided by reporters for the purposes of children's hearings. In all of these cases, provision is made in the appropriate legislation for access to be granted. In the case of adoption records, for example, details of a child's natural parents will be supplied only after the enquirer has been counseled concerning the implications of the request.

Similar provisions apply where the data indicates that the data subject was born as a result of IVF treatment as defined in the Human Fertilisation and Embryology Act, 1990. Such information is exempt from the Data Protection Act's subject access provisions but provision is made for it to be disclosed following the provision of counseling.

11.6 Failure to provide access

If the subject's request is not satisfied, an action seeking access maybe raised before the court. Here, it is provided that the court may order the grant of access except where it considers that it would be unreasonable to do so: 'because of the frequency with which the applicant has made requests to the data user... or for any other reason'. Assuming that a 1**10 access fee would cover the costs incurred by most users in satisfying access requests, it may be doubted whether this provision will be utilized to any extent. It has also been suggested, however, that a campaign of mass access requests might be used as a part of an industrial or other campaign directed against a data user. In the held of local government, for example, a spokesman for one authority has commented:

If there were a concerted campaign by some group and we suddenly had 5,000 applications arriving on the same day, we would obviously have a problem in providing the individual within the 40 day period provided by law.

Short of such unusual circumstances, it is difficult to envisage that a user will be able to rely upon this provision to refuse a request for access. It may also be the case that the vast majority of disputes between data users and subjects concerning entitlement to access will be resolved before the Registrar rather than the courts.

11.7 Matters arising subsequent to access

The possibility of obtaining access to data and of requiring changes to its contents has existed for a number of years in respect of files held by credit reference agencies. In considering '. the effectiveness of the rights and remedies provided in they Data Protection Act it is relevant, therefore, to make comparison with the relevant provisions of the Consumer : Credit Act, 1974.

11.8 Rectification of inaccurate data

The fifth data protection principle requires that personal data should be accurate. Inaccuracy occurs when data a 'incorrect or misleading as to any matter of fact'. In the ever the data subject alleges this is the case an action may be brought-before the High Court or a county court' seeking rectification or erasure of the affected data. The Directive will add the concept of 'blocking' of data, an option which may be appropriate where the processing of data 'does not comp with the provisions of this Directive'. If the action succeeds, it court may also order the amendment of any expression opinion which appears to have been founded on that data This approach contrasts unfavorably with the provisions the Consumer Credit Act whereby a procedure for rectification includes the possibility of requiring the Director General of Fair Trading to resolve any dispute between the parties. Th appears a more 'user-friendly' approach than one require that an individual institute legal proceedings although there always the option for a data subject of making complaint to the Registrar.

Particular problems have been identified in the situation where data has been received from a third party. Here the provides that such data will not be classed as inaccurate if marked as having been so received. In the event that the makes an accurate transcription of the data it is arguable that regardless of its inherent value, the data is an accurate representation of what the user has been told. Semantically, it is difficult to counter this argument. The danger with accurate records of inaccurate data arises when the record is to be used as the basis for action.

A report that an individual is a poor credit risk or has a police record may result in decisions being made adverse to that person's interests. Here, the Act shies away from requiring the rectification of the data held - which in the case of, for example, computer files of newspaper stories or books would come very close to rewriting history-but provides that the court may

require that the original record be supplemented by an account of the true state of affairs. Correction of inaccuracies in a file may safeguard the data subject for the future. It will be of no assistance where the information has been used or disclosed previously. Under the Consumer Credit Act, where a record is altered following a complaint from an individual, details of the change are required to be notified to everyone who received the erroneous data within the previous six months. No equivalent proposal is found in the Data Protection Act and subjects may be faced with the virtually impossible task of trying to track the movements of their personal data without being entitled to any assistance from a data user.

Implementation of directive should bring a significant and welcome change to this situation, it being provided that the controller will be required to provide notification of any changes made to the record to any third party to whom the data may have been disclosed. No limit of time is placed on this requirement although the obligation will not apply where notification would prove 'impossible' would involve 'a disproportionate effort'.

Rights to Compensation

Both Act and Directive provide for compensation to be payable to individuals who suffer loss as a result of certain forms of processing operations. The Directive's provision is broad requiring that :

> ... any person who has suffered damage as a result of an unlawful processing operation... is entitled to receive compensation from the controller for the damage suffered.'

The Act adopts a more compartmentalised approach providing rights to compensation in respect of three discrete forms of processing.

11.9 Compensation for inaccuracy

In limited circumstances the Act affords data subjects an entitlement to claim compensation in respect of inaccurate data. The right will arise where the inaccuracy has caused them 'damage and distress'. Damage is to be regarded as any form of financial loss while distress, in line with its normal meaning, refers to emotional upset or injury. The use of the conjunction 'and' entails that some element of financial loss is an essential requisite of .any claim. Even when the above ? conditions are satisfied the data user will not be liable if it can'

be established that all reasonable steps had been taken to ': ensure the accuracy of the data. Few instances have been reported of compensation being awarded under this provision.

The Thirteenth Report of the Data Protection Registrar reports an instance where a court awarded compensation of £ (pound sterling) 100 in respect of an inaccurate entry in a credit reference agency file although there is no indication what , form of damage was suffered by the individual concerned. The '' issue was also discussed in the case of Pascal v Barclays Bank plc. The case arose from a series of mishaps in the relationship between the parties cumulating in an error in the defendant's..:" records causing debt collectors to be instructed to recover fund from the plaintiffs.

The proceedings in the Court of Appeal were concerned with a variety of procedural issues but the Court considered also the various claims which might be open to the plaintiffs. Actions had been raised seeking compensation for malicious falsehood and negligent misstatement. The Court also noted:

What Mr. and Mrs. Pascal now foreshadow in their notice of appeal is a claim under the Data Protection Act 1984 which provides for compensation under a number of headings, in particular for compensation for inaccuracy under Section 22, and compensation for loss or unauthorized disclosure under Section 23. In both cases there is an express provision that the person who suffers damage, under one or other of those sections, shall be entitled to compensation from the data user, not only for that damage but also for any distress that the individual has suffered by reason of the inaccuracy. So, if there is a claim under the Data Protection Act it might result in a wider entitlement to damages than the damages, even if they are made good, for negligent misstatement where probably no claim for distress would be allowable.

It may finally be noted that, as suggested in Pascoe, the remedies established under the Data Protection Act are additional to any which might arise under any other branch of the law,. In the event that a contractual relationship exists between the parties it might be possible to point to either an express or an implied contractual provision requiring the accurate maintenance of records.

Dependent upon the nature of the information and error and the range of its dissemination it may also be the case that an action will lie under the law of defamation. In the case of credit

reference agencies, the view has been expressed that their activities are likely to benefit from the defence of qualified privilege. Although certain data users may also be so protected it may be doubted whether this will be so in the majority of cases.

11.10 Compensation for unauthorized disclosure

Compensation may also be sought for damage and distress occurring subsequent to the loss of data, to its unauthorized destruction or disclosure or to the unauthorized obtaining of access by a third party.' If an action for compensation is competent and the court is satisfied that there is a substantial risk of repetition of the conduct at issue it may order the erasure of the data.

The distinction between the concepts of 'loss' and 'destruction' is not clear. It would appear that the former term refers to the situation where data cannot be found and the latter to the situation where it is known to have been destroyed. The limitations upon the availability of compensation are broadly as described above. Once again, a defence is available that reasonable care was taken to prevent the loss, destruction or disclosure of the data or the unauthorized access. An even more significant limitation may arise from the fact that the question whether access, disclosure or destruction was authorized w ill be determined by reference to the state of mind of the data user rather than to the terms of the entry on the Register. If a data user determines to disclose data to a party falling outside the scope of the relevant Register entry he or she may face the wrath of the Registrar but will not be liable to the data subject no matter how much damage and distress the disclosure may have caused.

Effectively, the subject's right will only exist when the act in question is performed by an employee of the user acting without the user's knowledge or authority. Standing the prospect of action by the Registrar, it appears somewhat strange that what might normally be regarded as circumstances aggravating the gravity of conduct will instead constitute a defence. The comments made above regarding other forms of action which might be available to the subject will also be relevant in the context of an unauthorized disclosure of data.

11.11 Complaints to the registrar

Perhaps the most effective course for a dissatisfied data subject ,ill be to enlist the assistance of the Registrar. The Act provides in this regard that the Registrar shall consider any

complaint alleging a breach of any provision of the Act and requires action to be taken where the complaint appears to involve a matter of substance and to have been raised without undue delay by a person directly affected. In common with many of the provisions relating to the Registrar, this undoubtedly affords a considerable measure of discretion.

The discretion appears to have been exercised in favour of the data subject in the fulfillment of what has been described by the Registrar as his 'ombudsman' role. The Registrar's thirteenth report notes receipt of 3,897 complaints in the year 1996-97. In a significant number of cases the report indicates that the complaints have either been resolved in a manner satisfactory to the subject or have led to prosecution of the data user (generally on the basis of a failure to register) or the service of an enforcement notice.

11.12 Subject access in perspective

As with the exceptions to the non-disclosure principle discussed previously, any analysis of the subject access provisions must begin with the recognition that, save in very limited areas, no access rights existed prior to the enactment of the Data Protection Act. In many areas, the existence of a right of access to data held on computer has highlighted the incongruity of the absence of a similar right to data held in a more traditional format.

In the case of medical records, for example, it can make little difference to the nature and purpose of a record whether it is stored on a computer disk or in a manila envelope. Such considerations undoubtedly contributed towards the extension of the access rights with the enactment of the Access to Medical Records Act, 1990. In respect of the exemptions to the right of access, few would dispute that some forms of exemption are necessary and, indeed, desirable. A number of the provisions, however, appear to have been drafted in a fashion which will cause interpretative problems for data users-whilst, from the subject's perspective, a major weakness lies in the absence of any mechanism to monitor the operation of the exemptions.

11.13 Short Summary

- Much original detection will be conduced by police forces, a variety of criminal or quasi – criminal functions are exercised by other regulatory authorities.

- The fifth data protection principle requires that personal data should be accurate. Inaccuracy occurs when a data is incorrect or misleading to any matter of fact.

- In limited circumstances the Act affords data subjects an entitlement to claim compensation in respect of inaccurate data.

- It may finally be noted that, as suggested the remedies established under the Data protection Act are additional to any which might are under any other branch of the Law.

11.14 Brain Storm

- What is meant by Regulating of financial services?

- What is the role of Secretary of State?

- What is meant by cooperation for inaccuracy?

Lecture 12

Introduction to E-Commerce Law

Objectives

In this lecture you will learn the following

- Business to business e-commerce
- Business to customer e-commerce
- Cyber law
- The challenges of the information era digitalization
- The growing importance of information

Coverage Plan

Lecture 12

12.1 Snap Shot – Introduction

12.2 Meaning of electronic commerce

12.3 Business to business e- commerce

12.4 Business –to –customer e-commerce

12.5 Benefits of e-commerce

12.6 Risk of e-commerce

12.7 Cyber laws

12.8 Initiatives in India

12.9 Electronic commerce and the world trade Organisation (WTO)

12.10 The opportunities for company secretaries

12.11 The Challenges of the information era digitalization

12.12 Communication

12.13 Disaggregating

12.14 Impact on Business

12.15 Short Summary

12.16 Brain Storm

12.1 Snap Shot - Introduction

Scientists who figured out how to get computers to talk to each other thirty years ago, possibly had no idea that their work would evolve into the highly commercial, user-friendly Internet of today. Way back in 1969 the 'infant' Internet was possibly born, when a computer was first connected to a switch or routes and later to another computer. Many years elapsed before the concept took off in academic circles and more time still before the general public grasped the potential of a worldwide computer network. Internet has revolutionized society to enable users to search for material, retrieve it, store it on their computers and open it with a single command. The dramatic rise of the Internet and World Wide Web (www) has transformed the way business is carried out, improving accuracy, efficiency and speed. Thanks to the Internet, no longer is business restricted to limited geographical regions.

Today's industrial economy is evolving into a new business environment in which eg, goods, services and information are exchanged electronically. The Internet has thus thrown up unprecedented opportunities for even the smallest of businesses to compete with global conglomerates, while giving the bigger companies the possibility of reaching out further to its customers. With the digital revolution continuing and the Internet becoming more popular with each passing day, E-commerce has emerged as the fastest growing form of business today.

12.2 Meaning of electronic commerce (e-commerce)

E-commerce, means the ability to conduct business electronically, or over the internet. It is a generic term to describe technology-enabled communication with customers and suppliers for a business organization. When people talk about electronic commerce (e- commerce or EC), most will think of it as using the Internet to help the business market and sell its products and:-/or services. But in reality, E-commerce is much more than that. Generally, there are two kinds of e-commerce, business-to-business and business-to-customer.

12.3 Business to business e-commerce

The business-to-business kind of E-commerce refers to a company selling or buying from other companies. A company communicates with the other companies by electronic means:

This is actually not new, as many businesses have already been doing it since the 80's by means of Electronic Data Interchange (EDI).

EDI transactions include sending/receiving of orders, invoices and shipping notices. This is a method of extending the organization's computing power beyond its boundaries. But the high cost and maintenance of the networks made this method out-of-reach for small and medium sized businesses. In addition, the system is somewhat inflexible, as connecting a new vendor to the network would involve huge costs and restructuring. With the introduction of the Internet, companies, regardless of size, can communicate with each other electronically and cheaply. Companies that do so use it in several ways, depending on whether they are manufacturers or suppliers.

12.4 Business-to-customer e-commerce

The business-to-customer kind of e-commerce refers to a company selling its products or services to the customers using the Internet as the communication medium. This is what most people think e-commerce is about.

E-commerce isn't changing what happens in business transactions, but rather how they happen. Thus, e-commerce is the umbrella term for an entire spectrum of activities such as electronic data interchange (EDI), electronic payment systems, inventory and order management, product support and service, information delivery and the other business application linking solutions through the use of paperless information technologies such. as the Internet, bar coding, e-mail, smart cards, CD-ROMs, etc.

12.5 Benefits of e-commerce

Use of e-commerce technologies helps speed up the flow of information and to eliminate unnecessary human intervention; the computer can now accomplish what computers do better than people-process routine business transactions quickly and accurately, 24 hours a day. This in -turn, frees up people to handle tasks that computers may never be able to do-exercising judgment, creativity, and experience to manage exceptions, solve problems and continually improve business processes.

E-commerce is growing in importance and means unprecedented opportunities for everyone. When a business takes advantage of the power of e-commerce; if will be able to:

i. Increase customer satisfaction

The Internet is always open, even on holidays; business is thus always open, 24 hours a day, 7 days a week and 365 days a year. Customers will appreciate the extra access to product updates, shipping details, billing information and more. And since the Internet knows no boundaries, customers can shop from home, work, or anywhere they can make a connection. Besides, by connecting the e-commerce and shipping systems, it would be possible to ship products faster and for less money

ii. Increase sales volumes

The Internet is a new channel to reach new customers. With a Web site, a company can automatically become a global provider of goods and services, with an edge over even the largest competitors. Interactive selling is advantageous because a company is no longer limited by shelf-space or inventory concerns but instead offer all products to suit the customers' exact specifications.

iii. Decrease costs of doing business

E-commerce helps cut out or streamline processes that eat away profits. For instance, exchange of information from advertising to availability updates, can add to the cost of a sale. However, the web site can be an efficient, cost-effective communication vehicle. Customers can find timely, accurate information' in one place when they need it. By using e-commerce, everything from purchase orders to funds transfer can be handled faster and more efficiently. Even payment processing and bookkeeping are easier

12.6 Risk of e-commerce

As e-commerce evolves, it will present huge risks for those who don't take advantage of it. The main risk of e-commerce is that the business won't capitalize on all it has to offer, while the competition moves ahead. The traditional supply chain consists of the manufacturer, the distributor, the retailer, and the end consumer e-commerce is changing this linear view of the supply chain. Instead of goods flowing from one participant to the next, this new online marketplace can connect each participant with the end-consumer. For some links in the

supply chain, increased access to customers could be dangerous as partners could even become competitors.

12.7 Cyber laws

In the physical world today, there are requirements for documents to be in writing and for hand-written signatures.

Such requirements need to be translated into the electronic realm with the rapid development of electronic commerce in India; it has become expedient to amend existing legislation to facilitate the continued growth of electronic commerce and to resolve questions raised regarding the applicability of such legislation to the unique features of the electronic regime. The advent of e-commerce and the use of the digital medium as an alternative to the physical, have created some novel legal issues where there are no clear answers. .

The users of information technology must have trust in the security of information and communications infrastructures, networks and systems; in the confidentiality, integrity, and availability of data on them; and in the ability to prove the origin and receipt of data. For communication and transactions occurring over a faceless network, there is a need fur reliable methods to authenticate a person's identity and to ensure the integrity of the electronically transmitted documents.

The concepts of a secure electronic record and a secure electronic signature, and the rebut table presumptions that flow from that status, are thus necessary for a viable system of electronic commerce. In the context of electronic commerce, none of the usual indicators of reliability present in a paper-based transaction (the use of paper, letterhead, etc.) exist, making it difficult to know when one can rely on the integrity and authenticity of an electronic record. This lack of reliability can. make proving one's case in court virtually impossible. Rebut table presumptions with respect to secure records and secure signatures put a relying party in a position to know, at the time of receipt and or reliance, whether the message is authentic and the integrity of its contents intact and, equally important, whether it will be able to establish both of these facts in court in the event of subsequent disputes.

12.8 Initiatives in India

The challenge for lawmakers has been to balance the sometimes conflicting goals of safeguarding electronic commerce and encouraging technological development. On the initiatives of the Ministry of Commerce, initiatives a draft of Electronic Commerce Act and Electronic Commerce Support Act has been prepared to address the emerging issues in e-commerce and to create the legal framework for e-commerce transactions in India. An initiative in this regard has also been taken at the level of Department of Electronics which has drafted the Information Technology Bill (ITB) passed on l6th May 2000, which has been recently enacted and provided as an appendices to this book.

The Electronic Commerce Act aims to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions, the use of digital signatures and other issues related to electronic commerce.

The Electronic Commerce Support Act seeks to amend various Central Acts (viz. the Indian Penal Code, 1860;

the Indian Evidence Act, 1872;

the Contract Act, 1872;

the Indian Telegraph Act, 1885

the Banker's Books Evidence Act, 1891;

the General Clauses Act, 1897;

the Reserve Bank of India Act, 1934) to facilitate electronic commerce.

The Information Technology Act addresses contractual issues, computer crime and data protection. It also includes a section on digital signatures.

12.9 Electronic Commerce and the World Trade Organization (WTO)

Since 1998, WTO members have begun to explore how the World Trade Organization should deal with the question of electronic commerce. Given the unique nature of this emerging mode of delivering products (goods and services), many trade-related questions remain to be answered. For instance:

a. Under what circumstances should an electronic delivery be considered goods or a service?

b. When an electronic delivery is considered to be a service, under what circumstances should it be considered as crossing a border and under what circumstances should it be considered as being offered within the borders of a country?

c. To what extent is electronic commerce covered by existing WTO trade obligations?

d. How should electronic commerce be addressed in the context of future trade negotiations?

The broad consensus is that products which are bought and paid for over the Internet but are delivered physically would be subject to existing WTO rules on trade in goods. But the situation is more complicated for products that are delivered as digitized information over the Internet, as a variety of issues arise relating to the appropriate policy regime. Both the supply of Internet access services and many of the products delivered over the Internet fall within the ambit of the General ' Agreement on Trade in Services, but there is a need to clarify how far particular activities are covered by the members market-access commitments.

12.10 The opportunities for company secretaries

The role of a company secretary over the years has transformed from a mere legal compliance officer to a strategic integrated corporate manager. Foreseeing the growing impact of the global economy on virtually all businesses, company secretaries should take the lead to help facilitate international business transactions. Their professional education and training, combined with extensive experience in advising companies, representing clients in international business transactions, uniquely qualifies company secretaries to play a pivotal role in the next millennium. At a time when there is increasing focus gain the reputation of being top quality certification in international trade and commerce on win-win partnerships as a way to build sustainable businesses, it is important that company secretaries look at new techniques as a positive addition to the skills they can offer.

India will have to develop a public key infrastructure to facilitate the use of digital signatures. Under this infrastructure, the Certification Authority (CA), certifies that a given public key is associated with a given individual. The proposed legislation for e-commerce_ provides for the appointment of a Controller of Certification Authorities (CAs). The Controller will, amongst other duties, license, certify, monitor and oversee the activities of certification authorities. A licensed CA will perform a verification of the individual before issuing digital

certificates, in order to confirm the existence of all parties involved in an electronic transaction. This certificate can subsequently be used to confirm the public key of an individual, and verify the signature that is generated by the individual.

Maintaining operations and performing services in a trustworthy manner is fundamental to the integrity of the certificate and digital signature process. The certifying authority (CA), being in a position there will be public confidence in the services it offers. The company secretary, being a member of a body (the Institute of Company Secretaries of India) with a Code of Conduct, standardized training and other continuing controls, will be at an advantage.

The Institute of Company Secretaries of India should therefore, take the lead so that its members in practice can be... licensed to issue keys for digital signatures and act as:,; certification authority. The advantage for the company;; secretaries is that they already have a wide range of experience;:; in all types of business. With their knowledge, their intuition and ability to influence parties, company secretaries can gain the reputation of being top quality certification authorities.

The advantages are many. On a professional level, the work will be challenging, satisfying and better paid. The Institute on its part can conduct introductory and advanced training sessions by experienced and expert faculty so that a greater number of company secretaries in practice will have the opportunity to update and develop their skills. The Centre for Corporate Research and Training (CCRT) of the Institute can be in the forefront, to groom the company secretary prepare for this assignment so that they can meet the expectations of the beneficiaries of this service.

12.11 The challenges of the information era

Digitalization

Since computers operate in binary mode and recognize information only in digital fashion i.e. zeros and ones, we now see data, sound, images movies, ete., represented in digital form rather than in analogue form. This has had tremendous repercussions. For example, digitalization leads to perfect copies. Therefore, the millionth copy would be identical to and as perfect as the first one. Secondly, transmission of digital data is unaffected by distance so transmission across continents is as perfect as transmission next door.

Thirdly, copying has now become swift and virtually effortless. Piracy has therefore, become much easier and the control over Intellectual Property more difficult. Some interesting side effects of digitalization include the registration of trade marks for sounds such as the distinctive 3 rings of NBC Television and the distinctive roar of Harley Davidson motor cycles. In fact, digital representation of visual, auditory and olfactory phenomenon is expected to result in a bumper crop of new trade-marks appealing to the eye, ear and the nose. This itself will open up new vistas for trade and services marks unheard of before.

12.12 Communication

The computer is now more a communication tool than a computing tool. In fact IDC-the reputed and renowned firm-has predicted that by 2002, 50% of Internet access would be through non-PC devices. This means that the PC will look more like a telephone and be used like one to compete with economically priced non-PC tools which will be widely used for Internet access. In fad in a book titled "The Death of Distance" Ms. Frances Cairneross of the Economist has pointed out 30 major implications of the dramatic fall in world wide telecommunications prices and the equally dramatic rise in communication capabilities across the globe. These include the organization of work by global conglomerates into 3 phases based on the 3 major time zones namely the Americas, East Asia/Australia and Europe. Given India's huge and youthful population, relatively lower wages and educated English speaking workforce, it appears that India is superbly positioned to play a major role in the global services market through internet enabled services using satellite based telecommunication networks. Indeed such services promises to do for India what the mass manufacture of toys and electronics did for the Far East Asian Tigers. In fact Cairn cross echoes the famous economist Julian Simon in dubbing people as the ultimate resource and goes beyond that to emphasize that talented people would be a scarce resource. Suddenly given enough investments in education and training, India's vast population could become an asset instead of a burden.

12.13 Disaggregating

Leading consultancy firms and economists foretell the growing importance of specialization and out sourcing as the costs of interaction and transactions fall steeply. More functions and tasks will be outsourced to specialist organizations than ever before. Right from payroll

processing to valet parking services just about any activity appears to be outsourceable. In fact, the outsourcing almost all functions and keeping track of and coordinating outsourced activities.

12.14 Impact on business

The growing importance of information

Economies and corporations are now driven more by information than by any other factor. The well known US Economist Prof. Paul Romer has propounded a new growth theory of economics around information and innovations which seeks to explain the virtuous cycle businesses can attain through investments in R & D and innovation and the exploitation of Intellectual Property Rights. Labour, raw material and capital are becoming less and less important. As Mr. Peter Drucker points out the motor car has a labour and raw material content of 60% of its value. The microchip, which is ubiquitous and drives more devices each day, from satellites to washing machines, has a raw material and labour content of about 2% of its value. This illustrates the dramatic effect of information and IPR on businesses and the economy.

12.15 Short Summary

- The dramatic rise of the Internet and world wide web (WWW) has transformed the way business is carried out, improving accuracy, efficiency and speed.
- The business to business kind of E-Commerce refers to company selling or buying from other companies.
- The business to customer kind of E-Commerce refers to a company selling its products or services to the customers using the Internet as the communication medium.
- The main risk of e-commerce is that the business won't capitalize on all it has to offer, while the competition moves a head.
- Since computers operate in binary mode and recognize information only in digital fashion is zeros and ones, we now see data, Sound images movies, etc., represented in digital form rather than in analogue form.
- E-Commerce means the ability to conduct business electronically, or over the Internet.

- The business to business kind of E-Commerce refers to a company selling or buying from other companies.
- The business to customer kind of E-Commerce refers to a company selling. Its products or services to the customer using the internet as the communication medium.
- E-Commerce technologies helps speed up the flow of information. And to eliminate unnecessary human intervention.
- The Internet is a new channel to reach new customers and is always open.
- Department of Electronics has drafted the information technology bill (ITB) passed on 16th May 2000.

12.16 Brain Storm

- What is e-commerce?
- What are B2C and B2B?
- What are the benefits of e-commerce?
- What is the need of Cyber Laws?
- Explain the term WTO.
- What is A.E commerce and explain its kind?
- Give us the uses of E-Commerce
- What are the risks faced in E-Commerce
- What is a Cyber law? Explain the Imitative taken by our central government regarding this.
- Give us the impact of E-Commerce on business.

Lecture 13

Trade Marks and Service Marks

Objectives

In this lecture you will learn the following

- Trade Secrets
- Cyber Space and Cyber Laws
- Privacy
- The role of ICSI
- Emergence of Global E-Commerce
- The Electronic commerce transaction
- Creating a Binding commitment

Coverage Plan

Lecture 13

13.1 Snap Shot

13.2 Patient

13.3 Trade Secrets

13.4 Cyber Space and Cyber Laws

13.5 Issues and Recent Trends in Cyber Laws

13.6 The role of ICSI

13.7 Emergence of Global E– commerce

13.8 Types of E-commerce

13.9 Issues

13.10 Cyber Laws

13.11 The Electronic Commerce Transaction

13.12 Creating a binding commitment

13.13 Functional Equivalence

13.14 Short Summary

13.15 Brain Storm

13.1 Snap Shot

In a world in which technology products and services are proliferating, the only thing that is not keeping pace is human attention. In fact, Prof. Herb Simon calls this era the attention economy because attention is the scarce resource in the Information Age. This contrasts with capital as a scarce resource in the Industrial Age and labour as a scarce resource in the Agricultural age. Therefore, trade marks and service marks are becoming quite simply the most effective and indispensable way of attracting and retaining consumer attention,. in an economy in which millions of products and services are jostling for limited and scarce human attention.

13.2 Patents

Companies are furiously building up patent portfolios and preparing for patent wars as predicted by authors such as Fred Warshofsky In Prof. Warshofsky's words, where nations once fought for control of trade routes and raw materials, they now fight for exclusive rights to ideas, inventions and innovations.

Trade secrets

13.3 Trade Secrets

As Information proliferates and shoots across continents through the Internet the value of trade secrets keep growing. Encryption and security have attained newer meanings. Today company executives exchange secrecy and non-disclosure agreements as routinely as they earlier exchanged business cards before entering into any business discussions.

13.4 Cyber Space and Cyber Laws

The aggregation of Intranets (closed circuits of inter linked or networked computers) internet (world wide network of computers linked through various telecommunication links) and the world wide web (the networking of computers world wide with ready access to each others data through communication protocols and hyper text marked up language links) is dubbed as Cyber Space.

Cyber Laws, therefore, are those laws which have been adapted or re-interpreted to govern or apply to transactions or interactions in Cyber Space. Cyber laws also cover those special enactments which are specially designed to govern or apply to Cyber Space for example, the Electronic Commerce Act proposed by the Government of India or the Uniform Computer Information Transactions Act and the Uniform Electronics Transaction Act recently approved in the U.S for adoption by the various US States.

13.5 Issues and Recent Trends in Cyber Laws

Let us examine some issues and recent trends in Cyber laws.

Contracts

The Electronic Commerce Bill does promise to make electronic contracts feasible. However, we do need to learn from the experiences in other countries and to examine how our current contract laws could be applied to such contracts.

For example, would a supplier making details of goods and services with prices available on a website be deemed to have made an offer or would it be an invitation to treat as with a shop front display? Learned authors have opined that them is not much difference and; therefore, unless the website is so designed as to be construed as making an offer, in most situations, such displays would be treated in law as an invitation to treat. Some peculiarities may arise. For example, if the web site displays digital goods or services, there may be no scope for protection under contract law principles, on the ground that the possible depletion of stocks warrant the deeming of such displays as invitations to treat rather than offers. This is because there could be no depletion of digital goods which can be churned out effortlessly and in as many copies as may be needed, unless licensing restrictions apply.

The use of e-mails and web site offers and acceptances also present fresh challenges to current law on determination of the time and date of offer and acceptance. E-mails may not be actually received, just like the post, or be delayed or even lie unopened. On the other hand, web transactions more closely resemble telephonic and telex communications and offer and acceptance may be instantaneous.

Typical offences may be defamation or injury caused by the dissemination of computer viruses.

In the latter case, one needs to apply the usual principles used in determining who are legal neighbours arising from proximity, as also in determining the duty of care imposed on the defendant. On the internet legal neighbours may be in the next continent or next door. Also the duty of care differs based on the degree of control over the content and transmission of data to which the virus attaches itself.

Worldwide, anti-virus programs, test checks, audits of systems and log keeping of users are being used as methods of staving off liability for injury caused by the spread of viruses. Duties are also cast on the plaintiffs to use security measures, back-ups and their own anti-virus programs to defeat defenses of contributory negligence.

Privacy

In an issue titled, The End of Privacy, the Economist stated that "the volume of data recorded about people will continue to expand dramatically Disputes about privacy will become more bitter. Attempts to restrain the surveillance society through new laws will intensify." . . . "People will have to start assuming that they simply have no privacy This will constitute one of the greatest social changes of modem times."

The U.K. Data Protection Act of 1984, stipulates stringent rules for registration of personal data users and for regulation of the purpose, sources and use of such personal data.

In the U.S.A., the tussle is between the desire for personal privacy and the fundamental and cherished principle of free flow of information. In a paper called "A Framework for Global Electronic Commerce", President Clinton and Vice-President Gore call for the balancing of these two conflicting interests.

Domain Names

Recently, the Internet Corporation for assigned Names arid Numbers (ICANN) adopted a proposal for resolving domain disputes which will require mandatory arbitration of all such disputes involving trademarks, with the loser paying costs. This will become effective when adopted by Network Solutions

Inc., and other domain registrars and is incorporated in the appropriate contracts with domain name registrants.

Patents

The most profound and significant implications however appear to be in the area of patents. Two major areas here bear watching.

Firstly, both in the U.S. and in Europe more and more patents are being sought and granted for computer related inventions. In the U.S. the patent office has issued Examination Guidelines for Computer Related Inventions which have made possible the patenting of thousands of computer programs following the Beauregard matter in which the claim was for computer instruction fixed on computer readable media.

Secondly, in July 1998, the U.S. Court of Appeals has held that a computer implemented system for allocating investment gains and losses among a group. of participating mutual funds represented patentable subject matter, thus providing, what an expert calls, a definitive ruling on patentability of software related inventions.

The spate of such inventions which relate to the exploding worId of electronic commerce and the value of intellectual property is best exemplified by a company called Digital Walker which has about 12 such patents and over 240 patent applications in this area. The company is valued at several billion dollars within less than 2 years of formation and about half of its total staff of only 25 are lawyers with patent experience.

13.6 The role of ICSI

Company Secretaries, with their broad legal, financial and general skills are best equipped to take India and its entrepreneurs into the Internet world of commerce.

Here is what the ICSI can do:

- influence and help formulate a national e-commerce framework;
- create websites for exchange of views and debates on e-commerce laws;

- help create the 'soft' infrastructure needed; for example, insurance and liability advisories, funding and IPOs, venture capital networks, legal advisories etc.;

- permit and encourage foreign linkages for practicing Company Secretaries so that Indian firms can team more rapidly and create a global network;

- introduce specialized streams in the course for students in e-commerce laws and intellectual property laws

- review and seek changes in other laws which fetter e-commerce; set upon working group for this.

13.7 Emergence of Global E-commerce

The industrial revolution was perhaps the biggest change that businesses ever faced. In the beginning, we did everything manually, recording them on paper. Organisation maintained a clearly defined and often impenetrable boundary that separates them from the rest of the universe. In order to speed up the work we computerised it. Then we set up networks to share information pertaining to work. In our simple model of the business universe, the network first appeared within the organization. Interactions of the network with the outside world were almost zero. For any data to get added to or get out of the system, manual intervention was required. Someone had to take a printout and manually re-enter the data into a different network or copy it on to a floppy and carry it across. Hence interactions across the interface are often tirrie consuming and require elaborate processes and protocols. But in today's information age, this interface is rapidly crumbling and is being replaced by new mechanisms that make it easier to transfer Information across the boundary.

Electronic commerce is a modern business methodology that addresses the needs of organizations, merchants and consumers to cut costs while improving the quality of goods and services and increase the speed of service delivery using computer network to search and retrieve. information. E-commerce is associated with the buying and selling of information, products and services via computer networks. In other words, it is a means of transacting business electronically and in many cases over the internet. It involves a composite of technologies, processes and business strategies that foster the instant exchange of information within and between organizations, buyers and sellers. Information Superhighway (I-way)

will transform information transport technology for electronic commerce applications and provide an economic windfall. E-commerce is well suited to facilitate the current reengineering of business processes occurring at many firms. The broad goals are: reduced costs, lower product cycle times, faster customer response and improved service quality by reducing paper work, increasing automation. Today the emphasis has shifted from the narrow focus to the invention of entirely new business applications for reaching and getting close to the customer. New types of information based business such as on-line advertising and marketing, on-line order taking and on-line customer service which will reduce costs in managing orders, interacting with a wide range of suppliers and trading partners. E-commerce facilitates formation of new types of in formation based products such as interactive games, electronic books and information on demand, E-commerce will result in improved efficiency in finding and interacting with customers in communicating with trading partners and in developing new products and markets. Key element of e-commerce is information processing. Bottlenecks are long as transportation distances, customs regulations, language barriers etc. and coordinating them through software via the I-way can reduce the complexity.

Broadly speaking E-commerce is a new way of conducting, managing and executing business transactions using computer and telecommunications networks. E-commerce is expected to improve the productivity and competitiveness of participating businesses by providing unprecedented access to an on-line global market place with millions of customers and thousands of products and services. Another goal is to provide participating companies with new more cost and time-efficient means for working with customers, suppliers and development partners.

The traditional business environment is changing rapidly as customers and businesses seek the flexibility to change trading partners, platforms, carriers and network at will. Establishing private electronic connections to customers, suppliers, distributors, industry groups and even competitors to increase the efficiency of business communications to help expand market share and to maintain long-term viability in today's business environment. Traditional firms and financial institutions such as banks and credit institutions view electronic commerce with a mix of eagerness, fear and confusion. Many large and successful organizations fear that their vision on business no longer seems to apply.

E-commerce is the tool that leads to enterprise integration' for a company for an industry and ultimately for the vast network of small businesses, government agencies, large corporations and independent businessmen. An e-commerce site will enable one to extend the reach of his business by bringing in customers from previously untouched regions without incurring additional expenses of opening up branch offices or extensive and expensive advertisement campaigns. E-commerce has definitely not left India untouched though in India it still has a long way to go to before it matches international standards.

Many companies are pooling their resources and talents through alliances and mergers with other companies to make the electronic market place a reality. The term e-commerce has become irrevocably linked with the idea of convergence of industries centered on information. "Convergence" broadly defined as the meddling of consumer electronics, television, publishing telecommunications and computers for the purpose of facilitating new forms of information based commerce. Impact of convergence broadly includes: widening of the portfolios and building of existing customer relationships, creating opportunity and pressure to enhance delivery capability through services or products resulting in additions of more and more products supplementing each other in it, acquiring of small companies with innovative techn9logies by bigger ones to fill gaps in their product range, formation of strategic alliance in order to deliver complete integrated solutions etc. The whole process of convergence has been considerably slow because implementation requires large initial investment. Even the technology offered is still not a 'fool proof' one. All the networking majors are busy developing and acquiring various technologies to give converged networks to their customers. In this process very large and specialized companies have been killed in the name of acquisitions.

There are three compelling drivers that favour the emergency of converged networks. Capital savings. Operational savings and tariff savings. Seeing the recent market trend, service providers and equipment vendors are planning convergence, otherwise they are at risk of being sidelined and overtaken in the race. An important trend in the IT industry is the speedy change in technology. Convergence will be cost-productive for corporate with geographically spread offices.

Automating the flow of information and the process of decision-making help businesses substantially improve their time cycles, reduce inventories and generally improve the ROI.

Multimedia content can be considered both fuel and traffic for electronic commerce applications. Digital data in more than one format, such as the combination of text, audio, video and graphics in a computer file/document. Business professionals are well aware that more than 90% of the information that firms use for business operations and decision-making lives outside the "traditional" database systems. The goal of multimedia is to increase the utility of all information through the processing and distribution of new forms such as images, audio and video. Electronic commerce requires robust servers to store and distribute large amounts of digital content to consumers. These multimedia storage servers are large information warehouses capable of handling various content ranging from books, newspapers, advertisement catalogues, movies, games and x-ray images. Steady advance in digital memory technology are making mass storage devices technologically feasible and increasingly cost effective. All e-commerce applications follow the client-server model. In industries where the product or service is largely digital, such as banking, advertising, publishing, travel and entertainment, e-commerce will restructure the entire industry. e-commerce will enable new forms of products and services. and new ways of delivery.

Computers or information appliances that can log on to the internet are the very foundation of E-commerce. Till the usage of computers becomes wide spread, business-to consumer e-commerce can't realty flourish. If computer usage itself is insignificant internet usage is almost non-existent.

Internet is a global resource interconnecting millions of users based on a standard set of protocols-a mutually agreed upon method of communication between parties. It is slowly taking over the world of communication in a big way. Of course, the ideas different people have about the internet may differ but in fact it could be termed as the most powerful and important technological advancement. The dream of getting the whole world connected in such a way that information of any kind can be accessed and retrieved from any place has been ultimately realized through Internet. The FTTP (file transfer protocol) is a tool that allows transfer of files between I computers which in most cases would be connected over the internet. Similarly, e-commerce is the term that describes conducting business activities with associated technical data via electronic and telecommunication technologies over the internet. The internet has made it possible for business to; interact directly with both the suppliers and the end-users without having it go in for heavy investments with the use of Web browser and Web server. With internet, people no longer need to depend on radios as the only source to tune in to its individual stations. This is because web allow its audience to listen live from

various broadcasting stations. Internet can be leveraged to provide better customer service and tremendous time and cost savings. More companies are pumping their marketing dollars doing advertising and promotion via the internet.

Corporations saw the internet as a great way to put their sales literature on line. Number of web sites increased from zero in 1993 to over 4 million today which was better utilized by companies like Yahoo. Many companies are scrambling to connect electrical and electronic gadgets to the internet. Computer geeks are brimming with new ideas and researchers are competing to be the first to introduce new products or solutions that can provide such capabilities. Examples include kiosks, set-top boxes, technologies that enable mobile phones etc. People to talk to each other via desktops/laptops with internet connections. One day every electronic gadget that one carries or encounters in public will possibly have internet connection capabilities. There may come a day when publishing and advertising via one single medium the internet suffices for all.

With the collapse of geographical boundaries due to the evolution of the internet, ways of doing business have undergone a sea change. The trend is to have the applications web-enabled. This may be intranet, extranet or internet.

Now one could directly place an order on his supplier's network without any intervening paper work. This enables to plan better, reduce inventories, improve turnaround time etc. This is widely known as EDI (Electronic Data Interchange) system a fast and dependable way to deliver electronic transactions by computer to computer communication which is cost wise prohibitive particularly when a client and his suppliers are operating far apart. Next step is to extend the network to other customers which may not be practicable and hence to extend out to the distributor. Electronic Data Interchange forms part of e-commerce which operates viz. the transmission of paperless, computer- readable business documents electronically between trading partners and business systems. When a company shares its intranet with its suppliers and customers, they have in essence created an extranet. E-commerce is nothing more than financial transaction's that use information technology. E-commerce extends the value chain beyond the corporate boundaries and encompasses the full supply chain/product life cycle/sales cycle. It includes the use of information technology for EDI customer and product databases, electronic funds transfers, value added networks, interactive voice-response customer service systems, sales and marketing on the internet, electronic catalogs and basically anything simultaneously involving technology and business or e-commerce.

13.8 Types of E-commerce

E-commerce like the normal businesses that we are familiar with can broadly be divided into three types: Business-to-consumer, Business-to-business; and Consumer-to-consumer.
Business-to-customer sites requires huge investment not only W terms of the advertisement effort but also in terms of the hardware and software required to support the many millions of hits that they experience. For example, Amazon.com recently notched up ten million customers at its website and Ilediff.com claims a monthly hit rate of 40 million.

Business-to-Business (B-to-B) involves electronic business transactions between businesses. This typically involves transactions between trading partners-from largest companies to small and medium sized firms. The internet-has created a whole new way of implementing electronic commerce. Users will expect their business partners to use electronic commerce just as they expect them to use a fax and have a web site. In the users' opinion payment is not the most important part of electronic commerce. There are many opportunities for new applications.

The value of business-to-business electronic commerce to the user is greater accuracy, faster order processing, lower procurement and operational costs, better coordination among sales, manufacturing and purchasing, sellers become preferred suppliers when they offer electronic commerce, purchasers become preferred business partners when they use electronic commerce, the internet becomes an additional channel for sale, marketing and public relations activities.

Business-to-Consumer (B-to-C) involves electronic business transactions between a business and an individual consumer and is just beginning to emerge as a significant market. It is not as far advanced as business-to-business electronic commerce because the real growth of business-to-consumer electronic commerce is based upon the internet and the graphics oriented broadband world wide web portion of the internet. Business-to-consumer electronic commerce depends upon the interest of often fickle consumers, it is far more than credit card transactions. It include electronic catalogues, support and order status information.

The value of business-to-consumer electronic commerce for the business includes: extending the geographical reach of the business, allowing businesses to serve their customers seven

days a week and 24 hours a day. It is built around the internet which is an exciting new phenomenon for consumers the consumer does most of the work involved in entering and checking orders, thus saving the business time and money. Consumer accounts are already on the computer and thus they are easier to track for marketing purposes.

In industries that are consumer focused, such as retail, healthcare, telecommunications and some areas of manufacturing, vendors will take advantage of e-commerce to sell direct to the consumer e-commerce will impact the structure of product offerings and how they are delivered in the case of consumer-to-consumer they, don't form a very high portion of web-based commerce as these sites are auction sites.

In other industries providing support services to business such as logistics, transportation and some government services ices. The impact of e-commerce will be on marketing, selling and customer service.

Government-to-business electronic commerce, involves electronic transactions between government and businesses and helps both government and businesses to reduce costs and improves efficiency. Many also see electronic transactions with government as a means of reducing corruption and bribery. However, those countries that lag in the area of electronics will find themselves at a disadvantage in attracting investment and capital. In addition to businesses and individual consumers, governments are becoming a key player in electronic commerce. Governments and their citizens are also beginning to benefit from the speed, lower cost and efficiency of providing information and conducting transactions electronically. However, the real situation in South Asia except Singapore, is that in most countries only about one-third of the organizations surveyed answered "yes" as to providing data to government electronically. Those who availed the opportunity expressed benefits in the form of reduction in time and cost, fewer errors, quicker processing and turn-around and improved efficiencies Moreover, it was also noted that dealing with the government electronically dramatically reduces bribery and corruption. In addition, government itself stands to benefit from the improved efficiency and lower costs of electronic transactions.

Government-to-Citizen electronic commerce involves electronic transactions between government and citizens. Such transactions have already started in Singapore where citizens can file tax returns electronically. As the use of personal computers and the internet becomes

more pervasive across South Asia, governments will need to allow citizens to deal with government ministries and departments electronically.

13.9 Issues

The big issue facing e-trade is the absence of a clear-cut regulatory framework worldwide. India, with its complex regulatory framework needs to define transparent rules for e-commerce to keep pace with global growth. A number of issues like taxation, tariffs, data protection, authentication privacy and copyrights need to be reviewed from the e-perspective. This is a new challenge for lawmakers. E-trade dissolves boundaries a.-to brings in paperless dealings. Indistinct boundaries make it difficult to impose customs or other taxes on goods and services traded over the Net. If orders are booked on the Net but there is physical delivery of goods, taxation is possible. But how to tax a product that has been delivered over the Net-software constancy services or other information? Countries looking for alternative sources of revenues are planning to levy tariffs on global e-commerce. While trading, on the Net the seller needs to be sure that his intellectual property rights are protected. There are treaties that establish international norms for the protection of copyrights, most notably the Berne Convention for the Protection of Literary and Artistic Works.

Advertising: Advertising through television is costly compared to web advertising. Moreover, online advertising is more likely to be noticed than television advertising. Web users actively use the medium as opposed to passively receiving it. Few people actually pay full attention to television shows, not even two thirds of the viewers of television's most popular shows are paying "full attention" to the programming. Web surfers cannot navigate the web without high concentration and attention levels. Both are required for advertising to get noticed, remembered and ultimately acted upon.

Some of the concerns that need to be addressed relate to the area of taxation of goods and services traded via e-commerce. Tax treatment on such electronically traded goods under various tax levies such as customs, excises, sales tax, service tax etc. create problems. Although it is proposed to free all electronic transmissions from customs duties, what about taxing on such products depending on its mode of delivery.

Authenticity of a transaction on the electronic media is another concern. The identity on the Net is often anonymous, but how important is it to disclose the real identity? Another concern with authenticity is that there is no paper that holds; the stamp or signature of the parties involved during order; delivery or payment. Is such a transaction a contract. Does it' legally bind the parties who electronically enter into such an; agreement? Does not meeting the terms of the contract amount to breach of contract as stated in the Contract Act?

Issues like a customer denying that lie placed an order? online require sophisticated authentication mechanisms. It i not clear whether an authentication mechanism will recognized by an Indian Court as a valid evidence. Ethic legal mechanisms for such systems are required to succeed; otherwise customers in developing countries can get badly hurt.

Privacy is another important issue on the Net. Should an organization share the personal information that it collected beyond the extent that it was collected for? ECLIP (Electronic Commerce Legal Issues Platform) a committee set up by the European Union has laid down a legislative framework for privacy on the Net.

A lot of questions with few answers. There are no conclusive guidelines defined for these issues. There are international bodies, forums and commissions pondering on these issues to reach to an amicable worldwide solution. The fact remains that the issue is not in the hands of a single nation today. So, the attempt should be to have global legal standards, just as we have mutually accepted global technological standards. A government regulatory framework is a must to ensure smoother dealings, but in the electronic market place, a lot depends on the initiative of the private sector to create an overall environment of trust. Alongside, technologies like digital certification, encryption, user identification using retina prints or fingerprints, firewalls etc. also facilitate the provision of a safer environment.

Electronic commerce is an enterprise issue. Businesses today are faced with more competitive pressures than ever. They are under unrelenting pressure to reduce costs remaining responsive to both customers and suppliers. This pressure has driven businesses to recognize the need to automate and coordinate the flow of information between front-end and back-end of the business. Most of the organizations are integrating their existing enterprise applications with electronic commerce transaction capabilities to manage the flow of business transactions internally and externally across their customer and supply chain, become more customer - centric and, become what has been identified as the "next generation enterprise" i.e. one that

relates to its customers, suppliers and partners via electronic means. Therefore, enterprises today need to re-engineer themselves and their processes around electronic commerce in a similar fashion to the way that many enterprises have been re-engineering themselves around Enterprise Resource Planning (ERP) in recent years. Supply Chain Management and Customer Relationship Management are two electronic commerce related initiatives that have to be taken care of.

Banks and financial institutions stand to benefit enormously from e-commerce in the form of reduced transaction costs, improved customer service and loyalty and better customer information. They also get benefited from helping businesses handling payments and financial transactions by e-commerce.

Global Trust Bank Ltd. has entered into a strategic : alliance with Infosys Technologies Ltd. to facilitate its foray into electronic commerce by deploying Bank Away-a versatile platform for internet banking. Bank Away is a powerful electronic commerce platform that enables banks to provide an integrated financial services offering to their customers the one-click access to all their bank accounts, trade finance, bill payments and investments on line shopping and more. GTB plans to initially offer its customers a single view of all their accounts at any of the bank's branches. Customers will be able to know about their accounts and transactions, take print-outs of their statement of accounts, request for transfer of funds between their accounts, cheque books and demand drafts. GTB plans to offer value added services such as access to their trade ' bills, letters of credit and bank guarantees.

As far as Manufacturing compares are concerned, most manufacturers of the South Asian countries either directly or indirectly depend upon American and European markets"' which have fully developed e-commerce. Both South Asian a; well as Asian countries should fall in line with trading under e-commerce environment. There is a danger that too much expected from e-commerce initiatives unless they ensure "customer service improvement improved responsiveness and cost reduction". The imperative in the manufacturing sector today is to reduce costs in the fact of fierce global competition and over capacity. One particularly important area for cost reduction is in the supply chain. Taking expenses out of the supply chain could be achieved through e-commerce.

The timeframe for commerce on the Net can be divided into three, phases-e-commerce; e-business and E-service. The first two are over. E-service is the next phase. Which will see

intelligent interactions between E-commerce setups. Above all more than the technology or model, what is important is to understand how the business works and how it can be optimized to gain from going on line Thus, E-commerce has just started off and it would take more time to reach its full potential.

E-commerce will thrive by doing what is called disinter mediation. Dis-intermediation refers to the process of connecting the producer directly to the consumer and cutting out intermediaries such as brokers, dealers and the like. The underlying model of the new economy seems to be one where customers place orders with the company, the company processes the order and passes it on to a distribution point, which is in charge of getting the goods to the customer. Payment is electronic and directly from consumer to producer. In short, there seems to be little room for traders in this. The problem with this point of view is that it fails to take into accounts many other services that traders provide to the economy. Traders fulfill main functions that are indispensable to the smooth conduct of business. They help producers manage cash flows and inventories. Dealers are virtually the only customers of the company. The producer sells the goods to the dealer in bulk who plays for them and holds the goods till he manages to find a buyer. The company thus manages to get payments much faster than it would, if it were to sell goods directly to the customer. The management of inventory becomes the headache of the dealers as it is now off the books of the company. Doing away with this cycle would be prohibitively expensive for such companies. Similarly, intermediaries such as stockbrokers have a role to play in protecting the rights of the consumer. In the deal, if one party defaults in payment or delivers forged shares, the other party would have a tough time getting redress. It is mandatory that if a customer fails to pay then the customer's broker is forced to pay the seller's broker. The stock exchange has several "law making" elements but enforcing these is difficult by out connecting customers to brokers online would multiply complications.

Secure Electronic Records and signatures are afforded higher evidentiary presumptions to provide parties engaged in electronic commerce assurance that their transactions are enforceable. The security procedure must satisfy four criteria such as uniqueness, objective identification, reliability and linkage to record signer. It is presumed that the secure electronic signature affixed to an electronic record is the signature of the person identified as signer. If there is evidence that the person whose signature affixed was the victim of mistake, misrepresentation, duress or other invalidating cause, the record may be denied legal effect, but the burden of raising these issues is on the person denying the legal effect of the record. These presumptions apply only in a civil dispute and not in a criminal matter. A person

relying on digital signatures assumes the risk that the signature is invalid in circumstances where there is a questionable digital signature-one that cannot be verified because of several reasons such as an error by the signer or a faulty digital signature system.

Whether digital signatures on documents can be legally considered binding on the parties to the contract? How to avoid computer related frauds such as hacking, malicious falsification or erasure of data, software thefts, software attacks. Does require self-regulation by business community or through governmental intervention? Hence timely prevention and detection of Cyber crimes and frauds has to be considered. It is practically difficult even for the regulatory authorities in the developed countries to track down Cyber fraud relating to securities, such as frauds relating to purchase of securities through the internet money laundering etc. Instituting suitable legal changes and creating enforcement mechanisms are perquisites followed. by accountability by creating suitable technological standards for automatic monitoring of electronic payments and transactions. Detection of Cyber frauds and prosecution would also involve training police officials as well as prosecutors in advance technology apart from greater international cooperation between enforcement agencies. The International Chamber of Commerce believes that restrictions on cryptography failed in fighting crime.

13.10 Cyber Laws

In India, the absence of Cyber laws and methods of electronic settlement of financial transactions has constrained the growth of e-business. However, applications involving commercial transactions are not the only application in e-business. Applications with portals and Electronic Service Delivery (ESD) will flourish, while Cyber laws are getting formulated. Due to the non-existence of Cyber laws web-based business to-business commerce is based on an element of business risk. To encourage e-commerce in the country and to avoid confusion on tax paid on transactions, the government may consider not to charge sales tax on e-commerce transactions for a given period say five years. Cyber laws are vital to send a positive signal worldwide that Indian laws protect buyers, sellers and agents, while they do business on the network. Business-to-business sites are comparatively better off as they normally have negotiated contracts with governing laws and jurisdiction set out clearly. Also the transactions are normally between known entities that have or are actively looking for long business relationships.

The new government would usher in economic legislation with respect to introduction of derivatives trading Cyber laws and corporation of state electricity boards. Cyber laws' to govern e-commerce have been framed and are awaiting clearance from Parliament. Though transactions were being . done online, offline verifications were also being done to be on safer side. Safety measures should be in place so as to safeguard the system from illegal access, hacking etc. to protect the interests of the customers as well as the institutions. Cyber laws would also have to solve the taxation problems, creating an awareness among these people. Where physical verification would become difficult, in such cases the tax receipts of the government would be eroded. Although countries in Europe had finalized the Cyber laws in 1997, it took them two years to get these integrated in the country's economy. It is estimated that 4 lakh internet connections would be given by March 2000. The Ministry of Commerce has proposed a first draft for Cyber Laws which defines Cyber crime and lays down penalty provisions. The draft covers any act with willful intent to cause damage to computer systems and networks, spreading computer viruses and any act that is an offence under Indian Penal Code. The draft stipulates penalty for those found guilty of committing Cyber crime A first offence that does not result in damage carries a fine of Rs. one lakh or one year imprisonment or both. Subsequent offences involve Rs. two lakh or three years or both. If there is damage to any government or public properly, the fine would be Rs. five lakh or three years imprisonment or both. The draft also proposes to bridge the gap between the jurisdiction of two different countries in such a way that cyber laws of these countries have to have some elements of common understanding. Thus the Information Technology Bill to be passed by the Parliament by the year-end provides for authentication, evidence and recognition to electronic contracts and trade besides taking precautions against computer crime and for data protection paving the way for heralding an era of e-commerce in India.

The issues covered include consideration of the state of evolving business practices, suggested solutions to some recognized problems and a status report on the evolution of relevant legal standards. This chapter introduces relevant Legal principles, emphasizing the basics of contract and evidence law and their applicability to the creation and enforcement of binding commitments in electronic commerce. It will be seen how the current state of the law presents some uncertainties in relation to the formation and enforcement of agreements. We have also discussed the recent efforts and measures to reduce these legal uncertainties, including domestic laws, international conventions, guidelines and model agreements and provisions between electronic commerce participants.

13.11 The Electronic Commerce Transaction

Electronic transactions are conceptually very similar to traditional (that is, paper-based) commercial transactions. Vendors present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payment. Then, vendors deliver the purchased products. While the precise order of these events and the mechanisms through which they are transacted vary, these activities, are in principle, fundamental to both traditional and electronic commerce.

Nevertheless, because of the ways in which it differs from traditional commerce, electronic commerce raises some new and interesting technical and legal challenges. These include:

- Satisfying traditional legal requirements for reduction of agreements to signed documents;
- Applying legal rules of evidence to computer-based information; and
- Interpreting, adapting and complying with many other existing legal standards in the context of electronic transactions.

From a legal perspective, one of the most significant issues in electronic commerce is how to create enforceable digital contracts for the sale of goods arid services or how to ensure that a digital transaction will be at least as enforceable and valid as a traditional paper-based transaction. In every business environment, whether transactions are executed in person (face-to-face) or over distance, there are accepted customs and practices that determine, in conjunction with applicable legal rules, the parties, rights and responsibilities. These practices often include controls, such as:

- Signatures, to evidence agreements;
- Time and date-stamping, to provide proof of dispatch, submission, receipt or acceptance; and
- In some case, witnesses, notaries or other trusted third parties, to acknowledge and authenticate transactions.

The purpose of these controls is to create the necessary level of certainty in business transactions. Although electronic commerce is expanding rapidly, the development of a corresponding legal and control infrastructure has lagged behind to create viable electronic

equivalent to traditional contracting activities it is necessary to develop legal mechanisms or supportable legal analogs, for the electronic-commerce infrastructure. The goal of such mechanisms is to make electronic transactions at least as efficient, secure and legally binding as traditional commercial transactions, without forcing users to negotiate customized terms and conditions.

13.12 Creating a binding Commitment

At the heart of an electronic commerce transaction is the intention-indeed, the critical need-to form a legally binding agreement between the transacting parties. In this chapter, we introduce the legal principles of contract and evidence and examine their relevance to electronic commerce transactions. It will become apparent how the creation and enforcement of binding commitments in a digital environment depends upon adequate security measures and legal rules that recognize and reinforce these measures.

13.13 Functional Equivalence

The first question to be addressed concerning the law of electronic contracts is what law governs their formation, interpretation and enforcement. As noted earlier in this chapter, the law has been slow, in relation to the progress of technology and business practices, to accommodate differences between electronic commerce and traditional contracts. For the most part, parties to electronic commerce transactions have worked within the system of traditional contract law, making incremental adjustments to stretch and bend old legal principles to fit new business practices. Moreover, this trend is likely to continue, with certain exceptions, for two reasons: first, technology most often outpaces the law-legal regimes are, by nature, reactive-and second, electronic commerce has enough in common with traditional business that the traditional principles of basic contract and evidence law, within proper guidance, can usually be molded to accommodate digital transactions and govern them efficiently and appropriately

However, there are important differences between electronic and traditional commerce. For example, electronic transactions diminish reliance on paper to document a transaction and they also diminish the role of human participation in transactions. Nevertheless, these variations do not overcome the underlying functional equivalence between the major goals of

each type of transaction-both involve parties coming together to buy or sell goods or services, both involve payment and delivery and both involve the intent of parties to create a binding agreement and document the transaction for enforcement purposes. These functional similarities justify the currently prevailing approach of modest, incremental adjustments to traditional principles to accommodate many aspects of electronic commerce. Nonetheless, certain technical and business processes do vary considerably from traditional methods and, therefore, may benefit from more direct and comprehensive legal treatment.

13.14 Short Summary

- The electronic commerce bill does promise to make electronic controls feasible.
- The use of e-mails and website offers and acceptances also present fresh challenge to current law on determination of the time and date of offer and acceptance.
- The most profound and significant implications however appear to be in the area of patents.
- Company secretaries, with their broad legal, financial and general skills are best equipped to take India and its enter preheats into the Internet world of commerce.
- E-commerce is associated with the buying and selling of information, products and services via computer networks.
- India, with its computer regulatory framework needs to define transparent rules for e-commerce to keep pace with global growth.

13.15 Brain Storm

- What is meant by cyber space and Cyber Laws?
- What are the issues and recent trends in Cyber Laws?
- What the ICSI will do?
- Explain the emergence of Global e-commerce and its types?

Lecture 14

Sources of Law

Objectives

In this lecture you will learn the following

- Validity and enforceability
- Statues of Frauds
- Liability and damages
- Consumer issues
- Intellectual Property
- Legislation and regulation

Coverage Plan

Lecture 14

14.1 Snap Shot

14.2 Validity and Enforceability of Agreements

14.3 Offer and Acceptance

14.4 Consideration

14.5 Statutes of Frauds

14.6 Performance

14.7 Compliance

14.8 Breach

14.9 Enforcement

14.10 Liability and Damages

14.11 Evidence

14.12 Notice and Conspicuousness

14.13 Consumer Issues

14.14 Personal Jurisdiction

14.15 Negotiability

14.16 Intellectual Property

14.17 Illegal Bargains and Criminal Law

14.18 Dealing with Legal Uncertainties

14.19 Legislation and Regulation

14.20 Short Summary

14.21 Brain Storm

14.1 Snap Shot

The law that governs the validity and enforceability of a contract depends upon the choice-of-law rules of the jurisdiction in which an agreement's formation is formally disputed. Generally, in contract disputes, unless it can be proved that the parties agreed otherwise, choice-of-law rules mandate that the place where the contract was "formed" governs.

In both common and civil law systems, statutes and other legal rules assign legal significance to both the course of dealing between parties over time and to generally accepted and followed practices of the trade (usage of trade). Moreover, with certain exceptions, the parties themselves have the autonomy to agree upon principles to govern their own relationship, which may differ from statute and the common law. This approach ought to be undertaken particularly where the law would otherwise be ambiguous or uncertain. Accordingly, where parties to electronic commerce deal frequently with the same trading partners, they will often enter into trading partner agreements which establish ground rules for current and future dealings between themselves. 4Vhen they deal with infrequent or one-time partners, as is becoming increasingly common, parties ought to establish similar ground rules. Nevertheless, the practical limitation on negotiation in such instances urges the enactment of legislation and/or the establishment and recognition of system-wide rules or trade practices. The set of laws and rules governing a transaction may be summarized generally as follows and any inconsistency between them will, with certain exception, be resolved in favour of the higher set.

- Provisions of the agreement between the parties; - Course of dealing between the parties;
- Accepted trade practices in the applicable field of commerce;
- Pertinent statutory laws and regulations, such as the UCC (Uniform Commercial Code) and other legislative and administrative enactments; and
- The civil code of the jurisdiction or the common law as applicable.

The international business and legal community is serving to resolve a range of electronic commerce issues through developments such as the UN Model Law on Electronic Commerce. The work products of other international, regional or sectorial law-making entities have also influenced various aspects of digital transactions.

14.2 Validity and Enforceability of Agreements

An agreement between parties is legally valid if it satisfies the requirements of the law regarding its formation; that is, primarily, that the parties intended to create a contract. This intention is evidenced by their compliance with the three classical cornerstones of a contract an offer of specific terms, acceptance of the offer and adequate consideration (payment) for the performance of the agreement. Notwithstanding the validity of an agreement, parties may be unable to enforce a contract unless certain other requirements have been satisfied, such as the statute of frauds (where applicable), which is described below.

14.3 Offer and Acceptance

The bargaining process must satisfy two requirements to result in a valid contract: first, mutual assent as an expression of the parties' intent to contract and second, sufficiently definite terms. In arriving at such mutual assent and definite terms, the parties employ the mechanics of offer and acceptance. In most circumstances, the contract process is initiated by an offer. Offers are many and varied-offer to sell, offer to purchase and unilateral offers. An offer is "a manifestation of assent to enter into a bargain made by the offer or to the offeree, conditional upon a manifestation of assent in the form of some action (promise or performance) by the offeree". Offers contain conditional promises which must be accepted by a return promise (such as to sell and purchase) or an act (unilateral). The existence of a conditional promise is what separates an offer from an advertisement, price quotation or from providing information as part of preliminary negotiation.

Notice that traditionally there is demonstrable human involvement in the assent to the agreement, particularly with respect to the acceptance. In contrast, doubts about legal validity might arise in connection with the issue of assent (offer and acceptance), as in the example of a computerized inventory system of a retailer which automatically places an EDI order for a specific item when data from point-of-sole terminal indicate that inventory is low.

The Drafting Committee for Revisions to UCC Article 2 is considering a new section which would provide that a "contract is created .... even if no individual representing either party was aware of or reviewed the initial message or response or the action manifesting acceptance of the contract". In the meantime, courts can simply impute assent from the original human involvement in the programming of systems. Also, trading partner

agreements may be executed which satisfy assent requirements. Such questions implicate the laws of "agency" and the issue of whether one's computer can be that person's "agent" and can have legal authority to act on that persons behalf.

In an electronic transaction without the interposition of human interaction, both the offeree and the offeror must assent to the agreement contemporaneously. In all transactions, electronic and otherwise, the timing and legal effectiveness of the offers, acceptances and any revocations thereof affect the formation of a valid contract. Where both parties are in each other s presence, the timing of the offer and acceptance and the existence of any revocations are not in doubt. Section 64 of the Restatement provides that "acceptance given by telephone or other medium of substantially instantaneous two-way communication is governed by the principles applicable to acceptances where the parties are in the presence of each other". To qualify for this treatment, .a medium of communications must be capable of "prompt, reliable verification that a message has been received and that it has been received intact and without communication errors". The purpose of such techniques is the verification that the receiving party has had legally sufficient notice that an offer or acceptance has been made. EDI and other electronic commerce exchanges conducted on-line certainly satisfy this requirement, but delayed or store-and-forward communications such as e-mail may not.

A rule such as that set forth in Section 64 of the statement addresses problems with the so-called mail box rule-the legal principle typically applied in cases where parties do not use a substantially simultaneous communications medium. The mail box rule hinges legal effectiveness on the time of dispatch to as opposed to the time of receipt resulting in various anomalies.

Not only must both parties to a contract assent to. the agreement, but their assent must be to definite, specific terms and the acceptance must "mirror" the offer. Acceptances which fail to mirror offers in any significant manner may be considered to be new offers or counteroffers. These counteroffers may be in the form of a writing or a non-conforming tender of goods. In conventional contracting, because both vendors and purchasers frequently use their own standardized invoices and order forms the mechanics of offer and , acceptance often boil down to a battle of the forms in which each party sends its own form with terms which may conflict with those of the other party's form. To avoid needless hindrance of commerce, the UCC allows a contract to exist, notwithstanding non-material disparities and resolves differences in terms in favour of the offeror's form. Some commentators have claimed that

electronic-commerce heralds the obsolescence of such a rule because of its elimination of paper forms. This may not. be true since electronic commerce participants, particularly those without an ongoing relationship, may utilize their own standardized digital invoices and order forms, which may result in a digital battle of the forms. Nevertheless, under current law, parties to electronic commerce should be prepared to rely on the terms of the offeror's form or establish other ground rules through specific provisions.

14.4 Consideration

A valid contract also requires that the parties bargain for consideration. Consideration may consist of either actual performance, such as delivery of goods or services or payment for them or a return promise. Although electronic commerce may involve novel methods of payment and delivery, as long as a transaction includes a bargained for exchange of adequately commensurate promises or performances, regardless of the manner of performance, the agreement will comply with the consideration requirement.

14.5 Statutes of Frauds

Although a valid contract may be established through oral offer and acceptance, courts in the US and certain other jurisdictions typically do not enforce agreements involving various types of consideration unless they satisfy the statute of frauds; the legal requirement that 'some more or memorandum in writing' and 'signed by the parties' must exist for agreements of these types to be enforceable. The typical statute of frauds requires a writing and signature for the following classes of contracts, among others;

- Contracts of an executor or administrator to answer for a duty of his descendant;
- Surety ship contracts;
- Contracts made upon consideration of marriage;
- Contracts for the sale of interests in land;
- Contracts that are hot to be performed within one year from the making thereof; and
- Contracts for the sale of goods for the price of $ 5000 or more.

Thus, if an electronic transaction falls into one of these classes, parties seeking to create a binding contract must comply with the "writing" requirement and the "signature" requirement.

With respect to the writing requirement, the key issue is whether electronic commerce communications constitute written material for purposes of the statute of frauds. The UCC defines writing to include 'printing, typewriting or any other intentional reduction to tangible form'. This implies that other forms of communication might suffice. The fact that courts in the past have held that new modes of communication, such as telegraphs and telecopiers; satisfy the writing requirement suggests that courts will be similarly willing to adapt the law to digital media. A broader interpretation of the law may be required than was necessary for the novel media of the past since electronic-commerce does not, unlike telegraphs and telecopiers, necessarily involve a "tangible form". Nonetheless, the authors believe that the legal sufficiency of digital media will, due to the widespread adoption of digital techniques, increasingly be sustained where systems permit the production of a tangible record at any point when it becomes necessary.

Courts may be similarly flexible, as they have in the past, for new modes of communication, with respect to the signature requirement The Restatement provides that a signature may be-any symbol made or adopted with an intention, actual or apparent, to authenticate the writing as that of the signer. The UCC defines "signed" to include "any symbol executed or adopted by a party with present intention to authenticate a writing". Several possibilities might satisfy these definitions-answer backs, use of network access codes, message headers, including the sender's typewritten name at the close of a message and digital signatures. A digital signature is a cryptographic based mechanism that allows the recipient of a digitally-signed message to determine the originator of that message and to confirm that the message has not been altered since being signed by that originator. This mechanism, the operation of which depends upon the originator having sole possession of a secret data value called the private key.

Ultimately, the generous interpretations of courts may not be indispensable. Although limited to various circumstances, the US federal government has already blessed digital transactions involving federal procurement with full validity and enforceability-the Office of the US Comptroller General has stated, "Contracts formed using Electronic Data Interchange technologies may constitute valid obligations of the government for purposes of 31 USC 1501, so long as the technology used provides the some degree of assurance and certainty as traditional 'paper and ink' methods of contract formation."

Also, countries that choose to adopt a version of the UN Model Law would thereby provide for the legal effectiveness of digital communications with respect to writings and signatures, Furthermore, some US States have adopted legal reforms providing for the effectiveness of "electronic signatures" and electronic communications as signatures and writings. Other US States have enacted legislation giving, in varying circumstances, a communication that is "digitally signed" the same legal validity "as if it had been written on paper".

Provisions of the UCC Draft Televisions would accommodate digital communications in transactions by using the defined term "record" instead of "writing" and by broadening the defining of "sign" to include electronic signatures where proper authentication is available.

Such incremental changes would bring digital documents into legal compliance with the statute of frauds for the sale of goods.

The combination of judicial acceptance of new technology, the development of trade usage and legislative and administrative enactments suggests that electronically formed agreements will be found to constitute enforceable contracts for most statute of frauds purposes. Until legislation and trade practices become sufficiently uniform and widespread to provide comfort to parties in the jurisdictions in which they contract and otherwise conduct business, parties who wish a greater level of certainty for the time being should execute written trading partner agreements, thus, establishing more concrete rules.

14.6 Performance

Once a valid agreement has been reached, it is the duty of all parties to the contract to fulfil their end of the bargain; their efforts (and obligations to do so) are termed performance. Performance by both sides is, of course, what the parties have bargained for-obtaining performance is their object is forming the valid and enforceable contract. Thus, when one party fails to meet the legal requirements for satisfactory performance, there is a breach of the contract and non-breaching party may be entitled to certain rights against the breaching party Performance in many electronic commerce transactions involves electronic media, especially in the payments process or where the contract is for the provision of on-line services such as access to information or download of software.

Download of software and the access of billed information resources are examples of performance which can be completed without human mediation (beyond the initial programming).

14.7 Compliance

Theoretically a party's failure to perform completely and strictly in accordance with the terms of an agreement constitutes a breach of contract. Indeed, with respect to the sale of goods, the law has historically embraced the perfect tender rule, a standard entitling a buyer to reject goods unless the seller complies strictly with both quality and quantity provisions of a bargain. Nevertheless, where one party has substantially performed in good faith, it would frequently be unfair to force that party to forfeit all of his or her efforts simply because he or she has not fully complied with the contract. Thus, contract law softens the harshness of the perfect tender rule (or exact compliance) in some situations.

14.8 Breach

As stated above, a party's failure to perform as agreed results in a breach of contract. This includes both failure to perform according to the terms of the contract once the time "for performance has arrived and the refusal to perform even before the time for performance has arrived (termed anticipatory repudiation). Depending on the nature of the breach, a contract may be void on its face, void able by the ` non-breaching party or severable, meaning that certain term ` might be voided without affecting the validity of others. (In ' case of anticipatory breach, if the non-repudiating party has fulfilled its end of the bargain, the result is a total breach, giving rise to various rights on the part of the non-repudiating party, including the right to terminate the contract and make claims for damages.)

14.9 Enforcement

One of the fundamental objectives of contract law is to protect a party who accepts a promise in a properly formed agreement from injury as a result of a breach by the party who makes the promise. Accordingly, the law affords non-breaching parties various avenues of recourse to enforce their rights under the contract. Of course, a party who has been or stands to be, injured as a result of a breach must be able to prove the injury and the damages that flow

there from in court, under the applicable rules of evidence, to enforce these remedies. This section discusses the liability and damages a party might face for breach of contract and then addresses several rules of evidence that are particularly significant for the enforcement of contracts in electronic commerce situations.

14.10 Liability and Damages

A party which breaches an agreement may face various types of liability under contract law. In contracts for the sale of unique goods or other property, a plaintiff is typically entitled to specific performance of the contract by the defendant. An award of specific performance requires a court order demanding the defendant to deliver the goods or services to the plaintiff. Because specific performance is an extraordinary remedy, the capability to accurately identify the person whose specific performance is demanded is very important.

Where specific performance is infeasible or inappropriate, a court may award monetary damages to a plaintiff who has suffered injury as a result of a breach of contract. While various methods are used to set proper amount of damages depending on the nature of the breach, the goal of the law is generally to either restore the injured party to its pre-contract position (restitution approach) or place the injured party in the economic position it would have been in had the breaching party performed (expectation approach). This may include an award of incidental or consequential damages to compensate for expenses or losses attributable to the breach. Where a breach is committed in bad faith or through otherwise willful and malicious conduct, a court may award punitive damages. Parties may limit their exposure to liability for damages for breaches of contract by agreeing to clauses which liquidate or otherwise limit the amount of damages a party would be entitled to receive upon breach by the other.

Due to the nature of the systems and networks that business employ to conduct electronic commerce, parties may find themselves liable for contracts which technically originated with them but, due to programming error, employee mistake or deliberate misconduct, were executed and released without the actual intent or authority of the party. Sound policy dictates that parties receiving messages be able to rely on the legal expressions of authority from the sender's computer and thus be legally able to attribute these messages to the sender. Similar problems arise when transmission errors result in difficulties between parties, thus giving rise to damages. Some statutory proposal would prohibit parties (as between

themselves) from holding a third-party service provider or other intermediary liable for transmission errors or other omissions. These situations implicate the laws of agency, a set of principles governing the authority and legal capacity of an "agent" to act on behalf of its "principle".

The potential for liability due to statutory provisions for conclusive legal attribution provides additional incentive for electronic commerce participants to employ adequate security measures. In addition to employing information security mechanisms and other controls, techniques for limiting exposure to liability include:

a. Trading partner and legal technical agreements;

b. Compliance with recognized procedures, guidelines and practices;

c. Audit and control programmes and reviews;

d. Technical competence and accreditation;

e. Proper human resource management;

f. Insurance;

g. Enhanced notice and disclosure mechanisms; and

h. Legislation and regulation addressing relevant secure electronic commerce issuing.

14.11 Evidence

Rights and remedies are meaningless in the real world unless they can actually be enforced. Enforcement requires that a party prove, in accordance with the rules of evidence, that a contract existed, what its terms were, how it was breached and to what extent such party was damaged. For the contents of a document to be admissible in court, it must comply with several evidentiary standards, including: (1) the rule of authentication; (2) the hear say rule; and (3) the best evidence rule. Both courts and legislative bodies are currently attempting to deal with the application of these rules to computer based and other digital information. The key to admissibility of electronic commerce transactions and documents is evidence of data integrity.

A pre-condition to the admissibility of a record in judicial proceedings is its authentication, a requirement which is satisfied by "evidence sufficient to support a finding that the matter in question is what its proponent claims". Digital agreements, invoices and related electronic mail and other digital communications must be authenticated with respect to two aspects: (1) origin; and (2) accuracy of storage, retrieval and printing or other visual display. Due to the perception that "electronic files are particularly susceptible to purposeful or accidental alteration or incorrect processing", authentication of digital evidence may require, in some situations, a higher level of foundational proof than traditional evidence.

Authentication of a document's source is clearly related to the issue of compliance with the signature requirement discussed above.

Such authentication methods may need to involve a trusted third-party record-keeper, i.e., the use of certification authorities and notaries in conjunction with certificate-based digital signatures facilitates authentication.

Not only must a party seeking to prove the contents of a digital record establish the source of the record, but that party must also demonstrate that the current state of the record is accurate and has a proper chain of custody, that is, its systems of receipt, storage, retrieval and display does not result in deviations from the original message.

Under Federal Rule of Evidence 902, certain types of documents do not require extrinsic evidence to authenticate. These self-authenticating documents include official publications, public documents, newspapers and periodicals and acknowledged documents. Electronic documents with digital signatures may possess at least as much protection as these documents with respect to data integrity. Legal reforms should ultimately provide that certain digitally signed documents are self-authenticating. In any event, parties to electronic commerce must employ business practices, including adequate security measures, designed both to enhance and permit the parties to prove the integrity of their systems with respect to the receipt, retention and retrieval of digital agreements, invoices and all related electronic mail or other digital communications.

According to the "best evidence" rule, where there is any genuine concern regarding the authenticity of a "writing, recording or photograph", its content may only be proved by production of the "original" Federal Rule of Evidence 1001 which defines "original", provides that "if data are stored in a computer or similar device, any printout or other output readable

by sight, shown to reflect the data accurately, is an 'original'." Again, as with the authentication issue, questions may arise as to the integrity of the system and its ability to store, recall and print out or display an accurate version of the record. Parties should employ business practices which ensure reliability and permit the parties to establish reliability after the fact.

According to Federal Rules of Evidence 801, 802 and 803, "hearsay" or an out-of .court statement "offered in evidence to prove the truth of the matter asserted", is not admissible unless specifically allowed under an exception to this rule. Accordingly, electronic-mail or other digital communications regarding a party's understanding of contract terms or other relevant issues, is not admissible unless it can be shown to fall under such an exception. Most communications of this type, however, have the potential to be considered "records of regularly conducted activity", which are admissible under what is often referred to as the "business records exception". Case law confirms that computer data compilations are reliability of the records. To qualify, the records must be kept "in the course of a regularly conducted business activity" and as a "regular practice of that business activity".

However, the parties engaging in electronic commerce should seek to establish their own inter-party presumptions through trading partner or other agreements. For example, the Model EDI Training Partner Agreement stipulates that certain electronic documents "will be admissible as between the parties to the same extent and under the same conditions as other business records originated and maintained in documentary form" .

Other Legal Issues

Participation W electronic commerce raises various other legal issues. The following sections briefly address several of these issues. The list is not meant to be exhaustive, but merely to highlight and introduce some of the most relevant current developments and practices in secure electronic-commerce.

14.12 Notice and Conspicuousness

The accommodation of various requirements for legal notice and for conspicuousness via computer has been a source of continuing concern and uncertainty in electronic commerce. Traditional law and legal practice are premised on the use of the mails, the availability of

return receipts and other forms of confirmed delivery and on paper documents which permit large font type, capital letters and other conventions to call the recipients' attention to particularly important matters. Unfortunately, current legal standards provide no clear guide in this area.

In the absence of clear legislation, parties must establish precise meanings for notice and notify for each application. One possible requirement of notice should be the delivery of notification in a timely manner or within an explicit period of time. The legal articulation of "notice" should include whether it should or must be communicated via computer-based mechanisms or by other means, for example, certified or registered postal mail (and whether a return receipt should be requested) or a recognized courier service. The time at which notice is effective should also be defined; for example, upon receipt versus when it expressly comes in the intended recipient's attention.

When notice is sent electronically, the extent to which the recipient must verify its authenticity and acknowledge receipt should be determined. Because Internet e-mail does not support a return receipt or message confirmation service, the sender of an electronic notice may only request an acknowledgement of receipt from the recipient. Each party generally has an underlying obligation to exercise due diligence in maintaining system availability for electronic notice receipt.

If the notice's originator does not receive an acknowledgement of receipt within a specified period (such as two business days from the time sent), arrangements should be made to use an alternate mode of communications, such as first-class postal mail, certified mail or courier service.

In the revision process of UCC, various articles are seeking to articulate requirements for notice and conspicuousness that address computer-based commerce. For example, provisions in the current UCC Draft Revisions propose the following definition for "conspicuous:"

"Conspicuous" means so displayed or presented that a reasonable person against whom it operates would like to have noticed it or, in the case of an electronic message intended to evoke a response without the need for review by an individual, in a form that would enable a reasonably configured electronic agent to take it into account or react to it without review of the message by an individual. Whether a term is conspicuous is a question of law. Except in the case of an electronic agent, a term or clause is conspicuous if it is:

a. a heading in capitals in a record or display;

b. language in the body of a record or display and is in larger or other contrasting type of colour than other language;

c. conspicuously referenced in the body of a record or display and can be readily accessed from the record or display;

d. is so positioned in a record or display that the party cannot proceed without taking some additional action with respect to the clause, term or the reference to the clause or term or

e. readily distinguished in another manner.

The clause "without the need for review by an individual" may accommodate the use of diverse automated electronic commerce systems, such as those used in just-in-time manufacturing as well as certificate- based contractual extensions.

14.13 Consumer Issues

As electronic commerce continues to proliferate, consumers are becoming increasingly important participants. The law frequently provides added protections for consumers against fraud and unfair trade practices by unscrupulous merchants. The relative anonymity of parties in electronic commerce heightens the potential for such problems and the need for appropriate protection. Nonetheless, there has not yet been a major effort to reduce consumer risks in electronic - commerce from the recognized consumer advocacy organizations.

Moreover, the UN Model Law specifically notes that it does not supercede any consumer protection laws indeed the model simply does not address consumers. Current and proposed UCC sections take a similar approach by providing that UCC transactions are also subject to applicable consumer protection laws. The UCC and its proposed draft revisions rarely address consumers directly Despite the inaction to date, consumer protection advocates will inevitably respond to the challenges of cyberspace. One potential indicator of consumerism is the activism in the areas of privacy and data protection, in which new laws are being proposed and adopted with dramatic speed.

14.14 Personal Jurisdiction

Another legal issue of concern to those who engage in electronic commerce is personal jurisdiction or the ability to require others to answer to legal claims in the courts of a particular jurisdiction. US constitutional law requires that a defendant must have a level of "minimum contacts" with a jurisdiction to justify his or her being summoned there. In electronic commerce, messages relevant to a given transaction may pass through intermediaries in tens or even hundred of jurisdictions across the world-even without the knowledge or express consent of the parties. If the simple relay of a message through a service provider in a remote jurisdiction is sufficient to constitute minimum contacts, electronic commerce participants may be subject to enormous uncertainties. Until legal standards are crystallized in this respect, parties engaged in electronic commerce should agree upon jurisdictional issues in trading partner agreements or individual contracts.

14.15 Negotiability

The law has yet to address sufficiently the effects of electronic commerce on the negotiability of certain instruments which the law recognizes; as conferring rights upon their possessors. This type of documents include negotiable instruments, such as certain promissory notes and securities and negotiable documents of title, which include any "bill of lading, dock warrant, dock receipt, warehouse receipt or order for the delivery of goods and also any other document which, in the regular course of business or finance, is treated as adequately evidencing that the person in possession of it is entitled to receive, hold and dispose of the document and the goods it g covers". For example, a negotiable bill of lading is intended to " g adequately evidence that the person in possession of it is entitled to receive, hold and dispose of the documents and the goods it covers".

Because a paper record manifests recognized attributes of its originality and uniqueness, it possesses intrinsic legal value to its holder. However, digital documents do not possess an inherent uniqueness; indeed, one of their great advantages is their capacity for easy and precise duplication.

Since negotiability is an important commercial practice, electronic commerce participants must find methods of ensuring the negotiability of digital messages. To date, the only recognized methods that can provide adequate proof are the use of trusted repositories and the use of tamper-re5istant hardware such as smart cards. The UN Model Law makes some

progress in this regard by addressing contracts for the carriage of goods and providing the digital communications may suffice in certain circumstances as bills of lading and other documents of title.

14.16 Intellectual Property

Electronic commerce systems demand greater vigilance to ensure that parties do not violate or infringe upon existing copyrights, trademarks, patents or other intellectual property rights. In addition to copyright and trademark litigation, regarding the content of certain communications, there has been significant legal activity in the trademark area with respect to the use of Internet domain names. Some companies have registered domain names using the trademarks or trade names of their competitors. Network Solutions, Inc. (NSI), the entity that registers.com domain names, continues to struggle with increasing and novel disputes. In November 1996, an Internet International Ad Hoc Committee (IAHC) was constituted to consider various reforms to the current Internet domain naming system.

Although the courts have not, to date, distilled clear legal rules with respect to various intellectual property issues involving electronic commerce, including domain name disputes, parties have succeeded in obtaining definitive resolutions in certain cases.

14.17 Illegal Bargains and Criminal Law

While freedom of contract among parties to a transaction is the general rule, the law considers certain types of contracts as void or void able because of conflict with the public interest. The list of problematic contacts include those which unfair family relationship restrain trade or the "alienation" of property, involve promises to commit a crime or a tort (a wrongful act) or implicate commercial bribery. Although none of these types of illegal bargains are unique to digital transactions, electronic commerce participants should be aware of the potential invalidity or unenforceability of contracts against the public interest. Furthermore, various types of illegal subject-matter may cause particularly great harm within the electronic commerce environment, such as an agreement to traffic in pornographic or obscene material on the Internet. Parties who engage in some cases of illegal bargains may expose themselves to criminal liability.

Electronic commerce participants should be apprised of developments in the area of computer crimes. Even unsophisticated users have the ability to gain access to, use, misappropriate, alter or destroy information, records or communications, including sensitive payment information or trade secrets.

14.18 Dealing with Legal Uncertainties

As discussed above, legal principles demonstrate that there are many issues relevant to electronic-commerce which remain unresolved by formal legal systems. Because the most efficient solutions are often best implemented on a systemic or global scale, these uncertainties, if left untreated at a high level, will prevent electronic commerce from fully capitalizing on its technological efficiencies: Fortunately, policy-makers are progressing in some areas to recognize these issues and propose solutions.

14.19 Legislation and Regulation

Although policy-makers, in general, have not been quick to recognize the potential and inevitability of electronic commerce, certain legislators, regulatory agencies and domestic and international trade and legal organizations have increasingly focused attention on electronic-commerce law. Much of their efforts remain in the proposal or draft stage, but the trend is encouraging.

On a global scale, the most significant effort to address legal issues relevant to electronic commerce has been the UN Model Law on Electronic Commerce.

14.20 Short Summary

- The International Business and legal community is serving to resolve a range of electronic commerce issues through on model law or electronic commerce.

- Section 64 of the restatement provides that acceptance given by telephone or other medium of communication. Must be capable of prompt, reliable verification that a message has been received and that it has been intact and without communication errors.

- Consideration may consist of either actual performance or services or payment for them or a return promise.

- 'Some more or memorandum in writing' and signed by the parties must exist for e-commerce agreements.

- Once a valid agreement has been reached, all the parties to the contract to fulfill their performance.

14.21 Brain Storm

- What is a consideration?

- Give as some examples which requires awarding and signature for the valid contract?

- What is a 'Breach of Contract' in E-commerce?

- What are the liabilities and damages for breaching of E-commerce contract.

Lecture 15

UN Model Law on Electronic Commerce

Objectives

In this lecture you will learn the following

- Electronic funds transfer act and regulation
- Trading Partner Agreements
- Value-Added Network agreements
- The formalistic models
- The risk based models
- Digital Signature
- Legal minefields for Dot coms.

Coverage Plan

Lecture 15

15.1 Snap Shot
15.2 Electronic Funds Transfer Act and Regulation
15.3 Digital Signature Legislation
15.4 Guidelines
15.5 Forms of Agreements
15.6 Trading Partner Network Agreements
15.7 Value- Added Network Agreements
15.8 Interconnection Agreements
15.9 Payments Agreements
15.10 Security provision in model Agreements
15.11 Business Models
15.12 The formalistic Model
15.13 The risk based Model
15.14 Analysis of the Models
15.15 Business Controls in a Digital Environment
15.16 Legal issues : Indian scenario
15.17 Policy Guidelines
15.18 Conclusion
15.19 Digital Signature
15.20 Recent Laws on E-commerce in U.S.
15.21 Dotcoms, get the legal thing right or legit to the court.
15.22 Business Model
15.23 Legal Minefields for Dotcoms
15.24 Short Summary
15.25 Brain Storm

15.1 Snap Shot

A product of the UN Commission on International Trade Law (UNCITRAL), the Model Law is intended to advance the legal standing of electronic commerce by removing barriers to computer-based trade. Because no jurisdiction to date has adopted the Model Law as its own law; the Model Law is not binding upon any party to electronic commerce (unless its terms are specifically incorporated by reference in a trading partner agreement or other contract): Nonetheless; due to its precatory influence, the Model Law 'has greatly impacted the law of electronic commerce and the actions of participants in electronic transactions. An outline of the current Model Law is provided in the following Table 1 Part two of the Model Law is presently incomplete, but is intended to include "future additional provisions" to be drafted by UNCITRAL. Apart from this Model Law, UNCITRAL's next initiative relating to electronic commerce and communications will most likely be a Model Law or Digital Signatures.

15.2 Electronic Funds Transfer Act and Regulation E

The Electronic Funds Transfer Act (EFTA) governs the electronic transfer of funds or from consumer accounts within the jurisdiction of the US. Regulation E is the set of provisions which the Federal Reserve System has promulgated to implement the EFTA. As defined by the EFTA, an "electronic funds transfer" is "any transfer of funds, other than a'' transaction originated by cheque, draft or similar paper'.:. instrument, which is initiated through an electronic terminal; telephonic instrument or computer or magnetic tape so as to order, instruct or authorize a financial institution to debit or credit an account". In general, the EFTA and Regulation E provide consumer protection and allocate liability among electronic commerce participants, including financial institutions and the holders of physical tokens, such as ATM cards (or smart cards that possess ATM functionality). Thus, the EFTA and Regulation E provide an effective set of default rules for a portion of the payment aspects of electronic commerce.

Specifically, the EFTA and Regulation E impose requirements of disclosure and documentation, allocate risk for various mishaps and establish a dispute resolution scheme. In terms of disclosure, the EFTA mandates that consumers be apprised of their legal rights and remedies with respect to electronic funds transfers and the applicable charges thereof. Regarding documentation, the EFTA and Regulation E give consumers the right to receive documented information on each transfer and periodic statements of account activity.

15.3 Digital Signature Legislation

Various States and other jurisdictions have moved to give legal effect to electronic documents through digital signature legislation. Some States have enacted bills granting electronic signatures and electronic communications legal validity as signatures and writings, although it is unclear how effective such measures will be unless such "electronic signatures" provide at least similar levels of assurances regarding security, authentication, non-repudiation and other issues as those provided by digital signatures. Various other States have enacted legislation giving a communication that employs a digital signature the same (or greater) legal validity as if it had been written "on paper", detailing provisions regarding certification authorities, public-key infrastructure and apportionment of liability thereof.

Table 1 Outline of UNCITRAL Model Law on Electronic Commerce

		Part One Electronic Commerce in General
Chapter	I.	Genera! Provisions
Article	1.	Sphere of application
Article	2.	Definitions
Article	3.	Interpretation
Article	4.	Variation by agreement
Chapter	II.	Application of Legal Requirements to Data Messages
Article	5.	Legal recognition of data messages
Article	6.	Writing
Article	7.	Signature
Article	8.	Original
Article	9.	Admissibility and evidential weight of data messages
Article	10.	Retention of data messages
Chapter	III.	Communication of Data Messages
Article	11.	Formulation and validity of contracts
Article	12.	Recognition of parties of data messages
Article	13.	Attribution of data messages
Article	14.	Acknowledgement of receipt
Article	15.	Time and place of dispatch and receipt of data messages
		Part Two Electronic Commerce in Specific Areas
Chapter	I.	Carriage of Goods
Article	16.	Actions related to contracts of carriage of goods
Article	17.	Transport documents (Future Provisions)

15.4 Guidelines

Various sets of guidelines exercise increasing influence within the electronic commerce community. Guidelines provide an indication of usage of trade and possess the influence and authority of their sponsoring organizations. The guidelines described in this section exemplifv important contributions and initiatives.

The Uniform Rules of Conduct for Interchange of Trade Data by Tele transmission (UNCID), published in 1988, is the product of collaborative effort directed by the International Chamber of Commerce (ICC). Of great historical significance, UNCID constitutes a code of conduct or set of guidelines for EDI users, with specific focus on security and other communications aspects of trade data such as verification of a sender's identity, acknowledgement of receipt, confirmation of content, encryption or other methods of confidentiality and storage of data. In many respects, UNCID influenced the development of all of the early significant EDI trading partner agreements and legal principles.

With respect of future initiatives, the ICC is currently developing a set of Uniform International Authentication and Certification Practices (UIACP). The UIACP seeks to "integrate and harmonize the new digital signature legislation, the rich Latin material tradition in all its breadth and the wide-ranging law of authentication (signatures), including certified signatures, into a unified business standard for determining what constitutes a person's authentic act in a business transaction, whether by traditional, paper means or by electronic means".

Additionally, the ICC's ETERMS Working Party is advancing the ETERMS project-a registry of electronic commerce trade rules and provisions to serve both as a source for particular legal provisions and definitions which parties may specifically reference and incorporate into agreements and as a codification of standard, world-wide electronic commerce trade practices. ETERMS leverage the concept of the existing Incoterms programme of the ICC for traditional, paper-based trade.

The ETERMS project provides for the development and publication of diverse electronic commerce terms. In operation, ETERMS are intended to provide enhanced notice to and to

bind all contracting parties, within an international context. ETERMS include three kinds of terms:

- Commercial terms submitted by trading partners and information services providers;
- "Best Practice Rules" for electronic commerce; and
- Treaties, conventions and standards relevant to electronic commerce.

The ETERMS Repository can be remotely accessed and ETERMS can be incorporated by reference into trade transactions. The publication of an ETERM provides support for the notion that it has been adequately published and that users have or will be held to have, adequate knowledge of it.

15.5 Forms of Agreements

Agreements play an important role in electronic commerce. In the absence of a rich complement of relevant law and trade practices, including robust security standards, agreements serve to bolster the certainty of electronic commerce. The current extensive use of open systems increases the importance of agreements. Indeed; agreements provide a first fine of defence for parties trading over unsecure networks such as the Internet and with partners with whom long-term, trusted relationships have not yet developed (or where trust among the parties is otherwise marginal). On the other hand, where parties do not contemplate engaging in an ongoing relationship, negotiation of an agreement may be inefficient or impractical.

Agreements allow parties to benefit from freedom of contract. Without an agreement, the rights and obligations of; parties engaged in electronic commerce will be determined' (whether by design or default) by the prevailing law-which often differs from that parties' specific intentions and; expectations. Thus, even when legal rules in the electronic commerce areas are established with greater certainty, parties can use agreements to deviate from these rules when such deviation can use agreements to deviate from these rules when such deviation is to their advantage. In other words, agreements provide an important opportunity for parties to structure electronic commerce relationships that are consistent with their precise business needs.

Agreements can be classified as either (1) documenting a single transaction, such as the purchase and sale of goods or (2) providing rules to facilitate electronic commerce, such as those diminishing electronic trade barriers caused by traditional paper and hand-written signature requirements. Such facilitating electronic commerce agreements include trading partner agreements, Value-Added Network (VAN) agreements, interconnection agreements and payments agreements. These types of agreements are discussed in this section.

One model of the relationships involved in some of these arrangements is presented in Figure 1.

15.6 Trading Partner Agreements

Trading Partner Agreements (TPAs) are agreements between two (bilateral) or more (multilateral) parties who wish to trade electronically.

Such trading has traditionally been accomplished using EDI, but it now includes other electronic commerce methods for open systems, such as the Internet. Certain TPAs are sometimes called interchange' agreements, EDI agreements or pre authorisation agreements. TPAs can:

- Enhance the enforceability of underlying trade transactions;
- Reduce misunderstandings between parties;
- Apportion liability between trading partners, including liability for the acts of VANs or ISPs;
- Define the parties' confidentiality and security obligations ,
- Serve as an educational tool and implementation checklist; and
- Serve as an important audit and control tools.

Model TPAs have been prepared by the American gar Association, domestic and foreign governments and industrial and international organizations. Such TPAs attempt to provide a balanced treatment of legal and control issues, including at least a sub-set of the following issues.

Recitals: TPAs generally express the Parties' intentions to contract electronically and their acknowledgement that computer-based transactions are as valid and enforceable as comparable paper-based transactions.

Communication mechanisms: TPAs generally state which methods of communication the parties will use-such as VANs or ISPs.
System operations: TPAs typically state that each party must be followed to verify the integrity of messages upon receipt. They might also detail the actions to be taken upon receipt of illegible (such as garbled) information-typically retransmission or notification of the originating party.

Guidelines and user manuals: As a matter of course, TPAs will list applicable technical and procedural guidelines and implementation manuals.

Signature and writing requirements: Generally, TPAs win describe the nature and adequacy of signature substitutes (such as designated codes, authentication and non-repudiation security services).

Validity and enforceability: TPAs will usually declare the parties' intentions to create binding obligations using electronic commerce mechanisms. They also may state the admissibility and evidentiary presumptions with regard to such messages.

Security requirements: TPAs often require, the trading partners to use such methods as necessary to create enforceable transactions and to protect the confidential nature of inter-party communication.

Receipt : Many TPAs define what constitutes receipt. TPAs also often detail specific time parameters regarding when trading partners must check their e-mail in-boxes or send acknowledgements. Due to the lack of automatic, explicit message acknowledgements, this is particularly important for Internet-based transactions.

Acceptance : TPAs often state what constitutes legal acceptance and when such acceptance is deemed to occur for contract formation purposes. Many of the issues noted in the receipt discussion above are equally applicable here.

Battle of the forms: TPAs can provide a contractual solution to the problem of the "battle of the forms", in which, after the trading partners have reached agreement, one or both of the parties send additional terms, attempting to modify the agreement.

Record retention : TPAs usually identify which records must be retained in what manner and for how long.

Confidentiality : TPAs generally state whether some or all of the information communicated is intended to be kept confidential and under what conditions, if any, it may be disclosed.

Apportionment of liability : TPAs often apportion liability between the trading partners, including the acts of their respective third-party service providers, such as VANs.

Dispute resolution : Many TPAs specify whether disputes will be resolved through traditional channels (such as litigation) or through an alternative dispute resolution mechanism (such as mediation or binding arbitration).

Notice : Usually TPAs indicate where and how to send legally effective notice to the parties. Some TPAs also include provisions for electronic notice.

General boilerplate : TPAs also generally address issues such as assignability, severability, survivability, termination, governing law and force majeure (acts of god).

15.7 Value-Added Network (VAN) Agreements

VAN between a value-added data VAN agreements are executed communications service provider or VAN and a party desiring data communications services, typically for EDI. These bilateral agreements generally describe the data services to be provided, obligate the consumer to pay arid include warranty disclaimers and liability limitations. VAN agreements may also include technical information regarding the use and processing of formatted messages (such as EDI interchanges) and acknowledgements. These agreements also detail each party's responsibility for maintaining information security. The Internet Service Provider

(ISP) agreement is a variant of the VAN agreement. VAN agreements typically address the following issues:

Service description: A VAN agreement generally provides a description of the basic services to be provided by the VAN, such as data communications, EDI or other format translation and data mining.

Unauthorized access: A VAN agreement often states what constitutes authorized access and prohibits unauthorized VAN access with respect to both general communications services and certain value added services.

'Customer service: A VAN agreement typically states which customer support services are available, details of hours of operation, proper ways to communicate with customer service and maximum wait periods. It also distinguishes the VAN's regular customer service functions and services:

Ownership and use of customer data: A VAN agreement often describes the extent to which the VAN may use customer data. Perhaps, the greatest use in this area is aggregation of marketing data for resale by the VAN. VAN agreements also describe the extent to which a customer may obtain his or her archived data (including after termination of the agreement) and the fees VAN may charge for such services. They also state whether the customer can use materials and products supplied by the VAN following termination of the agreement.

Data retention : A VAN agreement often defines which data the VAN may or must retain and sets the retention period for defined types of data.

Availability : A VAN agreement generally states that the VAN must perform in accordance with its published user documentation. The provider also may guarantee that the system will be available for a specified time period (for example, 987 of the total hours for which services are contracted on a periodic basis).

Fees and surcharges : Fee and service provisions state which fees and services are chargeable to the user and establish the basis upon which such charges will be made (such as time and material, cost plus, etc.). Sometimes the VAN is permitted to adjust certain fees according to market conditions and inflation. The parties' respective obligations to pay taxes are also

sometimes included. When price increases are greater than a stated amount or rate, customers are sometimes permitted to terminate the agreements.

Termination of service : A VAN agreement frequently states that the agreement may be terminated without cause upon written notice by the service provider or customer within a stated time period or, in the case of default by either party, if such default is not cured within a stated time period, the agreement may be terminated.

Third-party audits : A VAN agreement sometimes states the right of the customer to obtain a copy of the VAN's independent audit report or to otherwise review the VAN's internal controls.

Reporting : A VAN agreement often states the obligations of the VAN to undertake various types of reporting, including, for example, system availability, customer access and use of data and system compromises.

Processing schedules : A VAN agreement sometimes indicates the frequency with which the VAN will process specified types of data or transmit data to other service providers.

Data recovering capabilities : Most VAIT agreements describe the VAN's obligations in the event of system failure or other problems that require contingency planning. For example, such provisions may guarantee the customer's access to a "hot" stand-by site or other backup facility detailing when, where and for how long.

Dispute resolution : In some cases, a VAN agreement sets the methods by which disputes will be resolved and the choice of Iaw or forum applicable to resolving disputes between the parties. Typically, the VAN will choose the courts within its local jurisdiction.

Apportionment of liability : A VAN agreement sometimes contains provisions, including disclaimers of warranty, for apportionment of liability between the VAN and its customer.

15.8 Interconnection Agreements

To facilitate reliable communications between trading partners connected to different VANs, many VANs interconnect their systems or networks. VANs execute interconnection

agreements with other VANs to state how their interconnections will operate and to protect themselves from liability. The precise terms of an interconnection agreement are a function of the parties respective bargaining power, business needs and technical protocols. These protocols vary in their capacity to communicate acknowledgements, transmit billing information and provide security. Interconnect agreements typically apportion liability between the VANs, indicate how and when data are to be exchanged and facilitate inter-VAN communications generally. Interconnection agreements typically include the following provisions:

Message transfer responsibilities : Interconnect agreements typically outline procedures and protocols for communicating trading partner data between interconnecting service providers. The provisions also specify whether batch data transfer will be communicated in a "send-only" mode, in which data are sent in only one direction or in a "send and / or receive" mode, in which data are sent in both directions.

Acknowledgements : Inter, connection agreements generally address acknowledgement, proofs of receipt of customer data and responsibilities for providing an audit trail. Data transfer acknowledgements take many forms, including negative acknowledgements, in which the receiving party notifies the sending party only if a problem is discovered and positive delivery reports, in which the receiving party acknowledges successful deliveries.

Error resolution : This provision addresses error identification and notification and resolution procedures. It generally indicates whether each party shall assist the other in responding to such inquiries; whether a fee will be charged for such assistance and whether the parties shall implement applicable operational and notification procedures. Responsibilities often, include resending data a specified number of times.

Level of service : Most interconnection agreements state the frequency with which each VAN sends customer data. This is particularly important for customers who have stringent timing and delivery rules as a result of interactive, on-line and other real-time business requirements. Typically, each party is responsible for billing and collecting its own charges from its subscribers.

Billing reimbursement practices : Interconnect agreements typically state how the parties shall bill and reimburse each other. Typically, each VAN is responsible for data it transmits to the other. The resolution of reimbursement issues becomes particularly important where

certain value-added services are provided, such as data translation between different EDI standard.

Charges and settlement procedures : This provision states the amount to be charged to subscribers for the interconnection services.

Apportionment of liability : Interconnect agreements often discuss duties of care among parties and address which party will bear liability risks in certain circumstances.

15.9 Payments Agreements

Payments agreements enable or enhance the certainty of success in making payments electronically. Payments agreements take various forms, including:
Financial EDI (or electronic commerce payments) agreements : These agreements are executed between trading partners. They state the responsibilities of the parties for making credit or debit based trade payments electronically Some of the issues addressed include the effect of partial payments, timing of payments and the use of funds clearing houses. Such forms of agreement are sometimes integrated into standard TPAs.

Credit card and Internet payment service provider agreements : These are agreements executed between a financial institution and a card or account holder.

Electronic Funds Transfer (EFT) Agreements : These agreements are executed between a financial institution and its customers. They typically define the rights and obligations of the customer and the bank and are associated with credit and/or debit-based electronic payments transactions.

15.10 Security provision in model Agreements

Since treatment of security in both domestic and international electronic commerce agreements has traditionally been quite modest, this chapter provides special focus on agreement provisions and related infrastructure supporting secure electronic-commerce. Examples of the information security provisions included within widely-recognized model agreements are:

Model EDI Trading Partner Agreement: "Each party shall properly use those security procedures, which are reasonably sufficient to ensure that all transmissions of Documents are authorized and to protect its business records and data from improper access".

Model Electronic Payments Agreement: "Each party shall employ reasonable security procedures to ensure that Transaction Sets, notices and other information specified in this Agreement that are electronically created, communicated, processed, stored, retained or retrieved are authentic, accurate, reliable, complete [and confidential]".

European Model EDI Agreement: "The parties undertake to implement and maintain control and security procedures and measures necessary to ensure the protection of messages . against the risk of unauthorized access, alteration, loss or destructiori ' .

None of these model agreements address how the parties should articulate their respective responsibilities for the implementation and use of information security techniques such as cryptography and digital signatures. Therefore, a new model agreement is clearly needed, particularly as business communication infrastructure migrates towards open systems, where trading relationships are increasingly new, parties do not necessarily trust one another and the use of digital signatures is advancing. A working group within the Information Security Committee of the ABA is now developing such a model agreement to articulate important information security principles and address security issues among trading partners and intermediaries.

15.11 Business Models

Molding traditional paper-based practices into practices appropriate for electronic commerce often proves to be a difficult task from the business perspective. For example, consider the uncertain kinship between traditional signatures and computer-based authentication methods. Most businesses have either purposefully or intuitively followed one of two alternative business models regarding signatures and authentication: the formalistic model or the risk-based model. The implications of making this choice are significant because the model chosen invariably impacts the type and strength of information security techniques, practices and procedures" implemented and the corresponding legal status of the digital information at issue. Each of these models is described below.

15.12 The formalistic Model

The formalistic model rests on two assumptions: first, legal requirements for both traditional and digital signatures are de minimis. Indeed, some experts claim that no security is needed to satisfy signature requirements such as statutes of fraud. Second, signatures and signature law are static and, therefore the security mechanisms necessary to satisfy signature requirements are also static. Thus, the formalistic model would dictate the use of the same procedures whether a transaction involves the low-risk purchase or the high risk sale to a questionable party in a developing, politically unstable nation with an uncertain legal system.

15.13 The risk-based Model

The risk-based model, on the other hand, rests on two contrary assumptions: first, there are inherent differences between traditional and computer-based signatures, requiring specific authentication and non-repudiation mechanisms. Second, signatures in digital commerce are necessarily dynamic and thus, must be commensurate with the risks of the subject transaction.

Thus, when the value of goods or the risk associated with a transaction is relatively low, the required controls are relatively minimal. But, when the value or risk is significant, the parties must implement more robust security mechanisms.

15.14 Analysis of the Models

The most significant pitfall of the formalistic model is that it fails to recognize that traditional, paper-based signatures have inherent security attributes that bolster their forensic utility, whereas computer-based information which is not specially secured does not. The forensic attributes of traditional paper-based signatures may include:

- The chemical bonding of a particular ink to a particular papers fibers;
- The biometrics properties of a signature, such as stylus direction, pressure and speed;

- The unique characteristics of a paper, including unique embossed letterhead, weight and style; or.
- A typewriter's or printer's unique fonts or a seal's unique die and wax.

In contrast, computer-based information has no unique forensic attributes unless supplemental artificial information security technologies, practices and procedures are applied. That is computer-based information is simply a series of zeros and ones that have no discernible uniqueness other than the content they apparently create. Therefore, there is clearly no simple analog between traditional and computer based signatures-not only because the media are distinct, but because the former enjoys critical inherent forensic attributes that the latter does not.

Under the formalistic model, where a single, static security/authentication procedure is adopted for all transactions, small risk/value transactions may result in unnecessarily large security/authentication (and unacceptable costs), whereas large risk/value transactions may enjoy lower security/authentication costs but will be inappropriately exposed to security compromise and resulting liability. Although the risk-based model involves an extra, incremental cost because it requires a non-standard response that must be tailored to each situation, it is more practical and efficient approach of the two.

15.15 Business Controls in a Digital Environment

Some of the most critical concerns of the secure electronic commerce community include the need to control liability exposure and the need to assure the enforceability of digital transactions. Although tremendous intellectual energy has been channeled into these issues, the community has notified comprehensively addressed the full range of critical issues in the larger electronic commerce control environment. At a minimum, guidance is needed to assist parties engaged in electronic commerce to identify, design and institute the business controls that would protect their interests and facilitate electronic trading.

Experience has demonstrated that there are no short-cuts to achieving secure electronic commerce. Rather, a rigorous, eclectic approach that weds technology to desirable and established business practices and procedures is required. Because electronic commerce is an

ever-changing field, it demands continuous oversight and proactive, creative innovation. Manager's must not only acquire the appropriate knowledge and resources and apply the proper management techniques, but must also invent or reformulate the appropriate control tools, techniques and procedures constantly. Such controls should, in turn, be reflected in electronic commerce agreements and trade practices.

As an example of the work ahead of electronic commerce participants in this regard, consider how an entity would undertake a risk analysis and security audit for electronic commerce practices, including those for an electronic commerce infrastructure that may have neither been fully built nor adequately tested. Adequate auditing tools and procedures for secure electronic commerce must be developed by proactively drafting them or by altering and extrapolating them from pre-existing audit programmes.

15.16 Legal issues: Indian scenario

Round one is finally over. Thank whole-heartedly, the much-awaited Internet policy is here. As one unwinds after the controversies, all those ups and downs, there is a feeling that good reason has triumphed over trivial pursuits of old monopolistic regimes.

Now the question is whether we can bet upon the new breed of ISPs to usher in a new era for India? Can the present euphoria be sustained? "Somewhere we go 70 per cent. And the last bit we seem to be forgetting. Unless the TRAI price recommendations are implemented, we don t see many ISPs surviving".

While the Internet policy, the basis of which is Internet for everyone, is in the right direction, ore needs to follow it up with implementation. The organizations which made it all happen-PMO, DOT, TRAI, IT Task Force, CII, FICCI, the media-cannot yet afford to take a back-seat. Who is going to see to it that the Grey areas that still remain in the policy get resolved? Who is going to ensure that the licensees do not have to wander about for clearances and for leasing resources like in the case of the other telecom services? Leased lines cost an astronomical sum and are still hard to come. Prospective ISPs like Satyam and ETH claim they are at least eight to nine times costlier than the rates in the US. To take telephone lines in bulk is still about doing several rounds of follow-ups with several telephone departments. ISPs do not have an option of using VSATs in the backbone, though they are available from several private USAT operators. It is true things change slowly in India. But, isn't it time we

started catching up? That DOT has licensed 21 ISPs in a span of 17 days as on 27 November is a good beginning.

This promptness has to be taken forward in lessening the paperwork, assigning resources for the licensees and looking at all possible ways to enable a fast roll-out of services. But if this is not happening, it is the responsibility of above mentioned organizations; to remind the authorities again and again by raising the problems in various forums and platforms. It is the high level of activism of various organizations and their concern of spreading the Internet which has made the big difference. There is no reason why this should not continue.

There are a few things more about which the drums have to be beaten. First is the issue of legitimizing the regulatory role of TRAI. If the Internet industry, for that matter any telecom industry, has to survive, TRAI's role as a regulator must be made stronger. In a situation where the rule makers are also the telecom service providers, a strong TRAI is a must. To make it simple, the powers of TRAI has to be made clear and as to have bearing upon all and sundry. The ruling of TRA should be binding upon DOT, MTNL, VSNL, also.

TRAI 'Soft ware recommendations on telecom pricing needs speedy implementation.

The recommendations according to ISPs, are extremely valid. If there are some concerns around the new set of price recommendations, they have to be ironed out between the various parties as soon as possible. Another point to note is that with so many players likely in the industry, disputes are bound to arise. All the more reason to strengthen the jurisdiction of TRAI. Another big task for the regulator would be to ensure a level playing field for ISPs. Today, the Internet scene is crowded. And everybody seems to have jumped into the fray. Evidently a large number of them being government bodies and public sector units like DOT, VSNL, MTNL, Railways, PGCIL and State electricity boards participation of these organizations; are necessary to speed up the penetration of Internet in the country and to fill in the gaps that exist in provide the various resources to the ISPs. But, let it not be that they have all the advantages in terms of resources and regulations while private enterprises are at their mercy for resources to run their business.

Only when the purpose is translated into action will the results be achieved. Going by the present government's agenda of transforming India into a global IT superpower, a lot more action-read implementation-will be needed before we can even come at per : with our

neighbours, leave alone the western countries. An encouraging step for the government would be to make the ISP industry an infrastructure industry.

15.17 Policy Guidelines

The government has paved the way for the privatization of Internet services by releasing the guidelines for the provision of Internet services. Key guidelines in the policy include:

Any company registered under the Companies Act, 1956 will be eligible to submit its proposal for operating Internet services to the Department of Telecommunications (DOT), the licensing authority.

Foreign equity participation to a maximum of 49 per cent will be allowed.

The country has been divided into separate service areas in three categories-A, B and C. Applications will be separate for separate service areas.

An applicant can be granted any number of licences and there is no limit on the number of licences that can be granted in a particular service area.

No licence fees will be charged till 31 December, 2003. However, licensees will have to submit a performance bank guarantee-of Rs. 2 crores for A-category, Rs. 20 lakhs for B category and Rs. 3 lakhs for C ISPs. After 31 December, 2003, ISPs licensed within this period will have to pay a token Re 1 licence fee per annum.

In accordance with the recommendations of the IT task force, interconnection between ISPs has been permitted. For international links, ISPs will be allowed to set up private international gateways after obtaining security clearance from DOT.

ISPs will also be allowed to build last mile linkages within their surface areas either by fiber optic or radio communication.

ISPs will be free to fix their own tariffs. However, quality of service is yet to be established and defined.

15.18 Conclusion

This chapter has considered certain legal and business principles relevant to electronic commerce, focusing on the validity and enforceability of electronic commerce transactions. A combination of certain tools, including agreements, legal and business practices and policies, security technologies, along with support for and refinement of these tools through legal reform, is essential to the success of electronic commerce. Legal requirements and business policies should clarify and implement reasonable security measures without sacrificing needed flexibility The past decade has witnessed great progress in developing the legal and security infrastructure necessary for conduct secure electronic commerce. Careful planning and rigorous attention to these issues will contribute to a viable electronic commerce environment in the future.

The inherent link between security and legal efficacy is not yet adequately appreciated. The security of electronic messages and records is not only a business requirement, but also a legal necessity. Defining this link is indispensable to the rational pragmatic development of reliable electronic commerce. The application of information security technologies, combined with an ever-increasing commitment to legal and business reforms, will result in increasingly more sophisticated and comprehensive legal and business practices and ultimately, in greater efficiency and benefit from electronic commerce.

15.19 Digital Signature

In today's commercial and digital world, technology develops faster than one can imagine and low struggles to keep pace. Electronic transactions will soon be the norm (if not already in some nations) and these transactions will lead to their own challenges, one challenge being to authenticate electronic transactions and messages. In the physical world, we use signatures and in the world of electronics, digital signatures shall play an important role.

To explain the importance of digital signatures one must understand the importance of a signature. A signature is not part of the substance of a transaction, but rather of its representation or form. A signature authenticates a writing by identifying the person who has signed on the signed document and thus acts as evidence. Signing a document also makes the

person signing aware of the commercial and legal implications of his act. Also, an important aspect of a signature is that it signifies the consent of the person signing the document to the contents of the document. A signature also indicates the finality of a document and one does not reed to question it or go beyond the face of a document.

Thus, keeping all these benefits of signature in mind, several types of transactions require signature by law. Lack of signature on a transaction or contract may make such transaction a contract unenforceable-in other words, avoid contract.

However, with the advent of electronic commerce, business transactions or contracts are being formed by new methods. The traditional ways of forming contracts are being slowly overshadowed by new electronic contracts the effect of which has caused the meaning of the word document to take a new perspective to include the paperless electronic form and the meaning of signature to include digital signature.

Digital signatures face two challenges in the electronic world. The first challenge is to authenticate the person who is signing the document so as to ensure it is executed by the person by whom it is claimed to be and the other challenge is to authenticate the integrity of the document itself so as to ascertain that it has not been tampered with or cause any alterations to the document to be detected. This will help in preventing forgers and impersonators from 'signing' the document and will prevent a person from unilaterally modifying an executed document without such modification being detected. Apart from these services, digital signatures also authenticate the origin of the document and with the help of other allied service providers help in authenticating the delivery origination and receipt of the electronic document.

The Information Technology Act, 2000 recognizes digital signatures in India and enables for its use. It has defined digital signature and provides for the use of digital signature to authenticate an electronic record (electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form).

The IT Act further lays down that there shall be a Certifying Authority who shall grant digital signature certificates to applicants. Such Certifying Authorities even have the power to suspend the certificate so granted.

To support and promote e-commerce and supplement the provision of the IT Bill, the Indian Evidence Act, 1872 ('Act') is also being sought to be amended. The definition of evidence is amended-to include electronic records. The terms digital signature, digital signature certificate, secure digital signature have also been included in the Act.

The Act shall further provide that the opinion of the Certifying Authority which has issued the Digital Signature Certificate shall be relevant in a court while adducing evidence in respect of on electronic document.

The IT Act shall also lay importance to secure digital signatures. It states that if a digital signature other than a secure digital signature is alleged to have been affirmed by any subscriber, such a digital signature would need to be proved.

A secure digital signature under the IT Act is a digital signature affixed by following security procedure as determined by the government. Such a digital signature should, on verification, be unique to the subscriber affixing it, be capable of identifying such subscriber and be created in a manner under the exclusive control of the subscriber and linked to the electronic record in such a manner that if the electronic record was altered, the digital signature would be invalidated.

Thus, for the purpose of evidence in a court of low in India, a 'secure digital signature' would be accepted without its validity being challenged. With legal aid being given to digital signature by the IT Bill and the proposed amendments to the Act; the use of digital signature to authenticate electronic transactions and contracts would soon be the norm.

In the buzz of e-commerce today, another killer 'app' on the Internet-e-mails shall also use digital signatures to authenticate communication.

Thus, if digital signatures are properly implemented, they will help us in a number of ways like preserving message integrity, minimizing the risk of undetected message tampering and forgery or false claims that a message was altered after it was sent; minimizing the risk of dealing with forgers or impostors or persons who escape responsibility by saying that they have been impersonated; and lastly, by retaining a high degree of security, information can be sent over open, insecure and inexpensive networks (like the Internet where your e-mail can actually be handled by other parties before it reaches the intended recipient).

15.20 Recent laws on E-Commerce in U.K.

1. Regulation of Investigator Power Bill: This Bill has , been passed in 9th Feb., 2000 and deals with three ' important areas: interception of communications, intrusive ', investigative techniques, and access to encrypted data:

2. Electronic Communication Bill: This Bill has been passed on l9th Nov, 1999 under this legislation:

- Electronic signatures will be given explicit legal recognition by the courts for the first time, giving people a secure electronic alternative to paper;
- obstacles in existing laws which insist on the use of paper will be swept away wherever it makes sense to give people the electronic option;
- a 'kitemarked' self-regulatory approvals scheme will be established to ensure minimum standards of quality and service. People will be able to check who has sent an electronic message, ensure it has not been tampered with and that no-one else has read it on the way (see Note to Editors 1);
- if-the self-regulatory scheme works, there will be no need to set up a statutory scheme. Only if self regulation failed would the Government establish a statutory scheme which would also still be voluntary. This part of the Bill will be subject to a 'Sunset Clause'. If a statutory scheme has not been set up within five years then the Government's power to set one up would lapse.

15.21 Dotcoms, get The Legal Thing Right or Leg it to The Court

Bubble or no bubble, the dot still fascinates. Few have survived the seductive lure of this little speck. The rush to set up dotcom portals continues unabated. The pot of gold at the end of a venture capital rainbow is still too strong a temptation. But a strange, dark phantom has now started spooking the dotcom opera.

And, the apparition that casts a pall over the dotcom phenomenon is of a legal nature. It's speciality: it can strike anytime, from any where. Content, contractual or service agreements, intellectual property rights (IPRs) all have to be made safe and secure from day one.

Most portals are too busy burning money-not their own of course, but provided by some munificent VC-to bother about legal niceties. People have to be hired, content has to be sourced, the host server needs to be tied up, direly needed eyeballs must be rustled up fast (since the second round of funding depends on that). Did you say legal due diligence? Get lost! Get me some more sticky eyeballs instead.

The portal (or, more likely, a web site masquerading as a portal) is now up and running. Your friends, cousins twice removed, neighbours all troop in through the portal once in a while to see what you're up to. And then, suddenly, bang!! Your get hit with a legal notice for something someone has put on the message board-offensive to 'public sensibilities' and requiring a painful trudge to the court. Or else, you've forgotten to register your trademark and you're now fighting a legal battle without any protective armor.

So, whether you like it or not, legal eagles are an indispensable lot for any net business, whether it is B2B or B2C. For those of you planning to set up new portals and without a clue about the legal jungle, here is a rough roadmap.

15.22 Business Model

A unique idea is guaranteed to get you the bucks. But if the business model is badly structured, spell trouble with a capital T. In a border less world, anyone can view your site, from any place. But that also means complying with laws, rules and regulations of a multitude of countries.

Rendering free financial advice on an investment portal may be the right marketing strategy, but better bone up on your cyber-history before doing anything of that sort... Generations ago-in cyber time, that is-financial advisers, who were registered with the Securities Exchange Commission (SEC) of the US, ran into trouble with UK's regulatory authorities. The reason: they had not registered with the British bureaucrats. The result: they couldn't peddle advice in that jurisdiction.

Later, the regulatory bodies of the two countries drafted a set of guidelines. Financial advisers of one country are now, by and large, exempt from registration in the other country. This extends to even web-based advertising. SEC has suggested that non-US financial services companies which advertise on the net should not be treated as infringing US regulations, provided these ads don't target US customers. Also, effective systems should be in place to prevent US customers from purchasing these financial products.

"There is no 'specific' registration requirement with the Securities and Exchange Board of India (SEBI) for providing financial advisory services. NRIs are a major market for the on-line broker-cum-adviser.

The should either abide by the regulations in other countries, which may include registration with the regulatory bodies or else they should disclaim that their services are meant for Indian residents only," explains Vaibhav Parikh, advocate with international law firm Nishith Desai Associates.

Source: Lubna Kably, Economics Times, 8 May, 2000.

15.23 Legal Minefields for Dotcoms

Potential e-customers can also become potential legal liabilities. For example, a bond issue may be invited subscriptions on the web. The application forms can be downloaded and payments made off-line. "If non-residents wish to apply, the onus of complying with the exchange control regulations must be on them. Such terms and conditions must be prominently displayed on the website," mentions Sridhar Gorthi, partner with law firm Singh & Gorthi.

Content Control

Content is the adhesive which brings sticky customers. Loads of content, and different kinds of content, bring in long term customers. But even this if fraught with problems. "The more the information which is accessible via the site, the greater the number of content providers, the more complex is the risk management process," says Harinder Lamba, advocate with Arnheim Tite and Lewis (a correspondent law firm of Price water house Coopers). The reason: content can accidentally defame a person or some of it may even be illegal in a few countries.

Rahul Matthan, partner with law firm Matthan & Ayappa, has an interesting observation: "Pornography is prohibited under applicable criminal law. The Indian Penal Code (IPC) can hold liable even those persons who put obscene work into streams of commerce." Parikh of Nishith Desai Associates supports this: "In fact, when a website containing objectionable content, is accessed from India, courts may hold that the owner of the site has committed an offence under the IPC. A grey cloud also hangs over adult chat sites."

Recently, the Washington Supreme Court, in the case of Lunney v Prodig Services, has held that internet service providers are not legally and financially liable when someone is defamed in e-mail communications or bulletin board messages. This case did not pertain to the web site owner and a question mark still remains.

Third Party Liability

Portals operating as facilitators of third .party transactions must clearly display terms of use, privacy policies and adequate disclaimers. Cautions Mr Gorthi: "Bid and buy sites, where users are free to come in and put up items for sale should be extremely vigilant about the goods." Pepper the site with sufficient disclaimers. This makes it abundantly clear that the website is a medium for communication, that it is not a party to the contract which users enter into and that the dotpreneur is not liable if the deal falls through for whatever reason.

Service Agreements

Sign a contract before getting married. Tricky issues crop up when relationships sour: who owns the website and the date? Who controls access to the site? Settle these before exchanging rings to avoid messy postmortems. Says Divya Bhatia, vice-president with Puretech Internet, a web-solutions company: "A website has two components, a front end and a hidden back end, which is the application (source code). The back end is generally not sold to the client (e-retailer), unless he pays a price for it." Says Mr Gorthi: "It's a matter of negotiation. A contractual agreement can be drawn up, whereby the source code is handed over as and when it is developed. The other alternative, appoint two development agencies, one to develop the web site and the other to check and hold copies of the code in custody." Even the front end, or the web design, is not free from dispute. Says Mr Matthan: "Copyright automatically vests with the author of the work, unless it was commissioned, in which case it

will vest with the dotpreneur who has commissioned the work." Legal boffins also suggest that dotpreneurs should draw up non-compete agreements to ensure that the same design is not drawn up for a competitor. But netetiqutte takes over when it comes to data.

Explains Divya Bhatia: "The data resides on my server, but we do not access the content on such web sites, unless we have obtained specific authorization to do so." The dotpreneur is charged for bandwidth. But failure to fork out cash could force the operator (who hosts the web site) to deny access to a web site. While no dotpreneur can do with a web developer, here is a word of caution. Philips India found to its dismay that the web developer had registered the domain name 'philipsindia.com' in its own name. When relationships turned sour, the company had to file a complaint with the WIPO to regain its rightful domain name.

Patents

Thanks to a profusion of patent suits in the US, the guys who've benefited the most are--you guessed it-the lawyers. Patenting is a self-consuming, obsessive craze in US today. Almost everything, even the smallest trivial detail, is patented, barring the view. Take Amazon.com, for example which sued rival Barnes and Noble over its 'express lane' ordering system-which only required a single click to process and order. In India, awareness is still lacking. No one has yet tried to patent a business model. Moreover, in some areas the laws have not kept pace with the cyber times. Software patenting is still not possible in India. But there are exceptions. An Indian company can patent software abroad if such software is not just 'pure algorithm just a formulae with no physical connection. Says Mr Parikh: "If a software controls a candy machine or even a key board (something physical) it can be patented in the US or EU member countries, but a pure calculation device cannot be patented."

Trademarks

Trademarks can be registered in India, but a service mark cannot be registered. The new Trademark Bill, 1999, which is still awaiting the President's assent, has, however, recognized service marks. India Inc, however, seems to have adopted a never-say-die approach. Software companies (which are essentially service companies), protect themselves by registering letter heads, printed manuals-anything and everything that bears their name. Or else, they take aid of a recent 'liberal' approach.

"Computer software which is sold on discs of floppies and which bears their logo can be registered under the Trademarks Act. This is not so in the case of software sold electronically," explains Mr Parikh. Registering all trademarks also helps give that extra leeway in protecting a domain name-or, your personal visiting card in cyberspace, if you will. "Recently Indian courts have accepted that domain names are capable of protection like any other valuable trademark," says Mr Gorthi.

Copyrights

Whereas patent law protects ideas, copyright protects only the author's expression of underlying ideas. Sources codes can be copyright protected under Indian laws. Since India is a signatory to the Berne Convention, copyright registration in India gives international protection. The Rights Management Information (RMI) is information that identifies the work, the author of the work, the owner of any right in the work, and any numbers or codes that represent such information. The WIPO Treaty makes it obligatory for signatories to provide protection against removal and alteration of any electronic RMI without authority. India has not yet signed this treaty. Thus, while it is mandatory to display particulars of the work and the copyright owner on the container while publishing any sound recording and cinematograph film, there is no specific provision on electronic rights, explains Mr Parikh.

Source: Economies Times, 8 may, 2000.

15.24 Short Summary

- The electronic funds transfer act (EFTA) governs the electronic transfer of funds to or from consumer accounts within the jurisdiction of the us.
- International Chamber of commerce (ICC) directed. The uniform rules of conduct for inter change of trade data. By tale transmission (UNCID)
- Trading partner agreements (TPAS) are agreements between two (BILATBRAL) or more (MULTIATERAL) parties who wishes. To trade electronically.
- Financial EDI (or Electronic Commerce Payments) agreements, credit card and Internet payment service provider agreements electronic funds transfer (EFT) agreements are various forms of payments agreements.

- An applicant for Internet services can be granted any number of licenses. That can be granted in a particular service area.

15.25 Brain Storm

- Explain guidelines regarding e-digital signature?
- Classify the different kinds of electronic commerce?
- Explain the uses of trading partner agreement?
- Explain the areas focused by van agreement?
- Explain the security provision in model agreement?
- Explain the forensic attribute of traditional paper – based signature?
- Explain the challenges faced by digital signature?

Lecture 16

Introduction to Cyber Crime and the Law

Objectives

In this lecture you will learn the following

- The legal response to computer hacking
- Limits of authority
- Application of the ulterior intent offence
- Logic bombs
- Operation of the Unauthorized modification offence
- Safety on the Internet

Coverage Plan

Lecture 16

16.1 Snap Shot - Introduction

16.2 The legal response to computer hacking

16.3 The computer misuse act

16.4 The concept of access

16.5 Limits of authority

16.6 Knowledge that access is unauthorized

16.7 The ulterior intent offence

16.8 The impossible dream

16.9 Application of the ulterior intent offence

16.10 Unauthorized Modification of data

16.11 Logic Bombs

16.12 Computer Viruses

16.13 The Legal Response

16.14 Modification in the Computer Misuse Act

16.15 Operation of the Unauthorized modification offence

16.16 Hackers sites

16.17 Safety on the internet

16.18 Short Summary

16.19 Brain Storm

16.1 Snap Shot Introduction

Crime involving high technology is going to go off the board was quoted by special agent Wilen Tafyo of FBT. Cyber crime is increasing leaps and bound with the increase of internet connectivity

The various types of cyber crimes are:

a. Phveakers
ii. Fraud

i. Hackers
ii. Pronography
iii. Viruses
iv. Pedophiles
v. Harassment
vi. E-mail security destruction
vii. Data didding
viii. Violation of privacy
ix. Crackers etc.

In this chapter we shall discuss in detail the Hackers activities and the legal issues related therewith.

Hacking is a generic expression in the computing world and can be applied in many contexts. In strictly computing terms, a hack is a quick fix or clever solution to a restriction. 'hack' is a temporary if ingenious fix or 'make do' rather than an attack on a system. Tricking a machine into performing an unintended task is the predominant characteristic of a 'hack', even well-known simple tricks such as sticking sellotape over pre-recorded audio or video tapes to enable reuse as a 'blank' tape can be described as 'hacks'.

In the popular, and in the legal mind, however, hacking has become unequivocally associated with the act of obtaining unauthorized access to programmes or data held on a computer system. This initial act is often followed by attempts to modify or delete the contents computer system. When, for example, the Communications Decency Act which sought to impose controls over the content on Internet sites, was being debated in the United States'

legislature, hackers secured access to the Department of Justice's WWW pages and replaced the department's logo with a pornographic picture.

More recently it has been reported that hackers accessed a web page associated with the Stephen Spielberg film, 'Jurassic Park-The Lost World' changing the title to 'Jurassic Duck The Lost Pond' and images of snarling dinosaurs into less threatening water fowl. Incidents such as these lend some weight to the notion that hacking is a relatively harmless phenomenon. Unfortunately, other forms of conduct can be far more damaging.

16.2 The legal response to computer hacking

At least before talk of the Millennium bug drove all other computer considerations from public attention, the activity of computer hacking received very considerable publicity. The stereotypical depiction tends to be that of a male teenager in a greasy T-shirt and torn jeans who spends hours slumped over a terminal, eyes gazing fixedly at the green glow of the VDU monitor. Banks, military installations, universities, companies and financial institutions fall before his relentless onslaught.

Nowhere is safe, no one can keep him out, no one knows of the scale of the threat, the silent deadly menace stalks the networks. Very often, how ever; as seen in the case of R v Gold, the reality is more prosaic. A recent discussion on the electronic 'hacker' Net News group a1t.2600 concerned the subject of hacking into the computerized legal retrieval service Lexis. For those hoping to reduce Lexis costs, the advice given was disappointing.

The best strategy suggested was to stroll into a local university and 'shoulder surf' a password from an unsuspecting user. This tried and tested method remains a favorite for those pursuing the intentionally darker side of 'hacking'. Many other 'hacks' are almost as quick and easy. During the Winter Olympics of 1994, the Net News carried many reports on how journalists had 'hacked' into the US ice skater Tonya Harding's e-mail account simply by using her date of birth. Consideration of the legal response to hacking prompted some of the most intense debates during the second half of the 1980s when the Law Commission's deliberations were leading towards the enactment of the Computer Misuse Act. There is little dispute that where the act of obtaining unauthorized access to the contents of a computer system is accompanied by further aggravating conduct such as deletion or amendment of data, criminal sanctions should follow.

As will be discussed below, it is arguable that this has been the position prior to the enactment of the Computer Misuse Act. The more controversial issue concerns the question whether the act of obtaining access to computer systems should, of itself, constitute a criminal offence. Here significant differences exist between the recommendations of the Law Commissions.

In its report, the Scottish Law Commission suggested such an offence should be committed only by a person obtained unauthorized access in order to inspect or otherwise acquire knowledge of the programme or the data or to add to, erase or otherwise alter the programme or the data with the intention either of securing advantage for themselves or another person or of causing damage to another person's interests; typically but not exclusively those of the computer owner.

Adoption of the Scottish Law Commission proposals would have entailed that the limited act of obtaining unauthorized access would not constitute a criminal offence. This approach was justified by the commission on the ground that, whilst much hacking was conducted with some ulterior end in view, many hackers, who:

> . . . are often quite young and possibly still at school, attempt to gain access to other people's computers simply because of the intellectual and technical challenge which that : activity presents. . . . Although we are not sympathetic to the view that unauthorized hacking should be encouraged so long as it is only a kind of intellectual game, we recognize that as a matter of public policy it is probably preferable to express any new offence or offences in terms which actually draw attention to the real mischief at which they are aimed.

A related point concerned the difficulty which might be encountered in sentencing an offence expressed in terms of unauthorized access of any kind. The analogy w as drawn to the situation existing in the area of road traffic law, where it has been held in both Scotland and England that a court should not, in passing sentence for an offence of careless driving, take any account of the consequences of the act. It was suggested that similar constraints would apply to an unauthorized access offence.

Other commentators also expressed the view that the mere act of obtaining unauthorized access should not be criminalised. The Data Protection Registrar posited the possibility of a hacker gaining access to a system with no intent of abusing its contents and who causes no damage'. Such conduct, he argued, was generally regarded as:

> ... juvenile 'hobby' behaviour. The Registrar recognizes the undesirability criminalising juveniles and the concern that young people should not introduced to the criminal justice system unless necessary.

Others have been much less sanguine in respect of the activity and it is fair to suggest that even a number of those initially in favour of a `kid glove' legal response have become more concerned at the implications of the behaviour as societal dependence on the technology becomes more and more extensive. A more stringent approach was advocated by the Law Commission and subsequently adopted in the Computer misuse Act. The Commissioners rejected the argument that the attempt to access a computer system out of curiosity or as a form of intellectual challenge posed no serious threat to the owners of the systems involved.

The Commission reported a number of cases where knowledge of the fact that unauthorized access had occurred led computer owners to expend significant amounts of time and about in checking or even rebuilding a system in order to be certain that no damage had occurred. A not untypical example of such a situation has recently been reported from the University of Cambridge and concerned the application of a practice referred to as 'packet sniffing':

> . . . 10,000 academics and students were now changing their passwords. 'Someone gained access to our system via the Internet and could have got to around 10,000 users files. The potential damage to Cambridge University and beyond is enormous.' . . The hacker used a so-called sniffer programme, which sat silently within the computer system for four weeks, monitoring its activities. This could allow the hacker to compile a list of all passwords to give him unhindered access to every computer on the university's network.

The cost and inconvenience involved in an incident such as this is substantial. It may be queried, however, whether the degree of solicitude expressed for the peace of mind of computer owners is replicated in other areas of the criminal law. If, for example, a house owner suspects that an unknown person has had possession of their keys and the opportunity to copy them, they may feel obliged to install new locks.

It would appear unlikely that in the absence of any attempt to secure entry to the premises involved, a criminal offence would have been committed by the other party. Again, if the operator of an airplane discovers that an engine casing has been opened by an unauthorized person they may well conduct extensive checks of the engine looking for evidence of damage.

It may even be that they would be considered negligent if they allowed the plane to fly without conducting an extensive examination. If caught, however, the perpetrator's liability will be limited to the act of opening the casing. In many cases it may be doubted whether this will constitute a criminal offence. A related issue concerns the question whether there should be a requirement that the computer user maintain adequate security measures (a requirement imposed under the Data Protection Act) in order to qualify for the protection of the criminal law against instances of unauthorized access.

In their recommendations as to the form of computer crime legislation, the Council of Europe advocated the creation of an offence involving 'the access without right to a computer system or network by infringing security measures'. Such an approach, it was suggested, would analogize computer hacking with burglary-style offences. Although the Law Commission report lays considerable stress on the security implications of hacking, stating:

> In our view . . . the most compelling arguments for the criminalisation of hacking are those stemming from first, the actual losses and costs incurred by computer system owners whose security systems are or might have been breached; secondly that unauthorized entry may be the preliminary to General criminal offences; and thirdly, that general willingness to invest in computer systems may be reduced, and effective use of such systems substantially impeded, by repeated attacks and the resulting feeling of insecurity on the part of computer operators.

The Computer Misuse Act does not require that any security measures be overcome. Certainly, access must be unauthorized, a point which will be discussed below, but the analogy may be with a person who ignores 'No Trespassing' notices and enters onto private property Save in the situation that their conduct is aggravated by other acts such as the removal of property, no criminal offence will be committed.

In Committee, an attempt was made to amend the Bill to provide a defence for a person charged under its provisions that 'such care as in all the circumstances was reasonably required to prevent the access in question was not taken'. In advocating this approach, reference was made to a press release issued by the Data Protection Registrar arguing:

> We should not lose sight of the fact that computer users ought to protect their own systems and, as regards personal data there is a duty clearly established in the Data Protection Principles. You've only yourself to blame if your neighbour's cattle get into your unfenced field.

The amendment, however, was rejected, one of the most telling objections being that it would be extremely difficult to make any assessment of what was to constitute reasonable care. The point was also made that English law has not recognized the concept of contributory negligence as a defence in criminal cases. A burglar, it was commented, could not demand an acquittal because his victim had left a window open.

16.3 The computer misuse act

The Law Commissions final report was published in autumn 1989 and recommended the enactment of a Computer Misuse Act. Unusually, the Report did not include a draft Bill, an omission explicable by the fact that it was believed at the time proposals for computer crime legislation were to be included in the government's legislative programme for 1989-90 and, therefore, that the report needed to be completed and published without delay. In the event, the Queen's Speech was silent on this point and in the absence of a government sponsored measure, a Bill seeking to give effect to the Law Commission's recommendations was introduced by Michael Colvin MP who had secured a high placing in the ballot for introducing private members' legislation. The drafting of the measure received a measure of support from the Parliamentary draftsmen but a number of cases brought under the legislation have highlighted definitional problems.

16.4 The concept of access

Merely sitting at a computer keyboard will not constitute unauthorized access. The first stage in the commission of the offence will consist of causing a computer 'to perform any function with intent to secure access to any programme or data held in any computer'. A variety of elements from this definition call for further discussion and comment.

Performing a function to secure access

This term is defined in such a manner that virtually any act involving use of the computer will suffice. Thus access will be secured to a programme or data when the user, by causing the computer to operate in any manner:

- alters or erases the programme or data;

- copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
- uses it; or
- has it output from the computer in which it is held (whether by having it displayed or in any other manner). Although the above provisions are somewhat tortuous

(and are themselves subject to further definition in the Act), it seems clear that most actions whereby a user makes contact with a computer system and causes that system to display or to transmit information will come within its ambit. Thus the simple act of switching on a computer will cause various messages to be displayed on the screen, whilst the act of making contact with some external system will cause some form of 'log in' screen to be displayed.

To a programme or data held in an computer

The basic offence requires that access be sought to any programme or data held in any computer. In order to commit the offence, it is not necessary that the unauthorized user should direct their attention at any particular computer system or seek to inspect any specific programmes or data held in the system. The effect of this provision is to render liable to prosecution those hackers who, perhaps by dialing telephone numbers at random, seek to discover those which serve as the gateway to a computer system.

The location of access

The popular image of a computer hacker is of someone who accesses computer systems by making a telephone connection from their own computer. This perception caused considerable problems in the first prosecution brought under the Computer Misuse Act. The case resulted in the accused being acquitted of charges under the Act on the direction of the judge. This was based upon an extremely restrictive interpretation of the scope of the unauthorized access offence.

The case was referred to the Court of Appeal by the Attorney General, where it is reported as A-G's Reference. The defendant in this case had been employed as a sales assistant by a wholesale locksmith. He left their employ but subsequently returned to the premises indicating the intention to purchase an item of equipment. Details of sales transactions were entered into a computer terminal. The defendant was familiar with the use of the system and,

taking advantage of a moment when the terminal was left unattended, entered a code into the system. The effect of this was to instruct the computer to give a 70% discount on the sale.

The invoice which was subsequently generated charged the sum of £204.76 instead of the normal price of £710.96. Upon these facts coming to light, the defendant was arrested and charged with an offence under the Computer Misuse Act. At trial, the judge dismissed the charge, holding that the phrase in Section 1(1)(a) referring to obtaining access to 'any programme or data held in any computer' required that one computer should be used to obtain access to a programme or data held on another computer.

Given the evidence from the Audit Commission surveys to the effect that most instances of computer misuse are perpetrated by 'insiders' and the fact that most computer systems are not accessible from outside, such a restriction would severely limit the application of the statute. The Attorney General, acting under the authority of the Criminal Justice Act, 1972 sought the opinion of the Court of Appeal on the question whether:

> In order for a person to commit an offence under Section 1 (1) of the Computer Misuse Act, 1990 does the computer which the person causes to perform any function with the required intent have to be a different computer from the one into which he intends to secure unauthorized access to any programme or data held therein?

Delivering the judgment of the Court the Lord Chief Justice answered this question in the negative. There were, he ruled:

> . . . no grounds whatsoever for implying or importing the word 'other' between 'any' and 'computer', or excepting the computer which is actually used by the offender from the phrase 'any computer'.

Such an approach is in line with the recommendations of the Law Commission which stated that whilst:

> 'hackers' are quintessentially thought of as outsiders . . . (i)t is in our view important to ensure when settling the terms of an offence that it is directed at unauthorized users of a system or part of a system, whether outsiders or insiders, that one does not concentrate exclusively on outside hackers.

During the Committee stage of the Computer Misuse Act's passage an amendment was unsuccessfully moved which, by substituting the word 'another' for 'any', would have produced precisely the result attained through the trial judge's interpretation. This amendment provoked strenuous objection from the Bill's sponsor, Michael Colvin MP, who argued that:

> The key issue is that unauthorized access to any computer system undermines the so-called integrity or trustworthiness of that computer system. One of the Bill's principal aims is to guard against that. As I said, so much of the hacking is carried out by insiders that to remove them from the effect of the Bill's provision would render it especially defective.

All available empirical evidence lends support to this argument.

To a programme or data held on a computer

One further point deserves consideration as relevant to all of the offences established under the Act. No attempt is made to define the word 'computer'. This is very much in line with the approach adopted in other statutes (such as the Data Protection Act) operating in the area. The offences, it will be recalled, relate to dealings in respect of programmes or data and may be triggered by an act causing a programme to perform its function. Many modern appliances make extensive use of simple computers, often consisting of a single semiconductor chip, to control their functioning.

A washing machine may, for example, have its operation controlled by such chips, whose circuitry will contain the programmes necessary for the performance of their dedicated tasks. In such a situation, it might be argued that an unauthorized person who used the washing machine might be guilty of the unauthorized access offence. Such a prospect was identified in Parliament, where it was welcomed by at least one MP who in opposing proposals to amend the offence to restrict its scope argued:

> This is a computer misuse Bill. It seeks to tackle unauthorized access to computers which may well include electronic locks. . . Someone breaking into a car using an electronic key to operate the lock may not be caught under the present legislation if a policeman puts his hand on his shoulder before lie gets in and tries to drive away. We are attempting to make it an offence for people to gain unauthorized access to an electronic system. The clause is properly drafted.

Such a result would appear not a little bizarre and if it were to be endorsed by the courts would put the unauthorized access offence in conflict with the recommendations of both Law

Commissions that the unauthorized use of a computer should not, per se, be made unlawful. The vast majority of computer operations, it may be assumed, will be conducted by the computer owner or with his knowledge and consent and will raise no issues under the Computer Misuse Act. Liability will arise only when the access is unauthorized and where the party responsible is aware that this is the case.

16.5 Limits of authority

The question whether access is authorized can be determined only by reference to the intentions of a party entitled to determine such matters. Thus access is held to be unauthorized when the user:

- is not himself entitled to control access of the kind in question to programme or data; and
- he does not have the consent to access of the kind in question to programme or data from any person who is so entitled.

In many cases the person entitled to control access will be the owner of the computer system itself. In other cases, a computer system may serve as a `host' providing storage space and access facilities for programmes or data controlled by other parties. In this situation, the question who has the right to consent to access may be more complex.

Most university computer systems provide illustrations of this form of activity. Here, the fact that a student is granted rights of access does not confer any entitlement to transfer these on to a third party. From the perspective of the controller of a computer system, the major impact of these provisions will lie in the fact that the unauthorized access offence will be committed only when a user is aware that access is unauthorized. In the situation where the controller makes no attempt to bring restrictions to the notice of users and applies no form of security, it may be difficult for a prosecution to succeed.

16.6 Knowledge that access is unauthorized

The question whether a particular use by a particular user is authorized will be determined by reference to the state of mind of the computer owner or any other person entitled to control access to programmes or data held on a computer system. In order for an offence to be

established, however, it must be proved that the party obtaining or seeking to obtain access to any programmes or data knew that this was not authorized.

The restriction of the statute's application to the situation where an accused acted intentionally might be contrasted with the Scottish Law Commission's recommendation that the prosecution should have to establish that an accused person acted recklessly. As has been stated previously, however, the mere act of obtaining access to programmes or data would not have been sufficient to constitute the offence. Enhancement of the burden of proof might be seen as the, quid pro quo for the enhancement of the scope of the offence.

Establishing intent

Establishing intent may prove a difficult task. In a recent case involving a prosecution under the Computer Misuse Act a jury acquitted a defendant who had admitted to obtaining unauthorized access to numerous computer systems. Although no reasons are given why any jury reaches a particular verdict, it would appear that they may have accepted the claim by the defence that the accused was addicted to hacking and, therefore, acted under a form of compulsion rather than with intent, notwithstanding directions from the judge that this would not constitute a proper defence to the charges.

> The case is described in Charlesworth, 'Addiction and Hacking', 1993 New Law journal 540. The accused, Paul Bedworth, had been charged with two other individuals with various counts of conspiracy to commit offences under the Computer Misuse Act. The two other defendants, perhaps to their subsequent regret, pled guilty and were sentenced to terms of imprisonment.

Beyond the rather dubious point whether addiction might destroy the capacity to form an intention, a number of real difficulties may be anticipated in applying this provision. In most cases, the initial act of making contact with a computer system will not suffice. Even though a hacker dialing telephone numbers at random (or making use of a number supplied by a fellow enthusiast) may well suspect that their attentions may not be welcome, and be reckless whether this would be the case, it may be very difficult to establish that they had actual knowledge that access was unauthorized.

A further scenario might also be identified. User A 11a been allocated a password by the computer owner. A discloses this password to B and encourages B to use the password to obtain access to the computer. It is likely that B's access will be regarded as unauthorized as although A is entitled to access the computer he is not entitled to 'control' access.

The question which may require to be determined by a court is whether B could possess the necessary evidence for commission of the unauthorized access offence. The dividing line between reckless and intentional conduct may well be crossed at the time access is obtained to a computer system.

A user accessing the main computer system at the author's university is presented with the message 'Unauthorized access to this system is ILLEGAL: Computer Misuse Act 1990' . The mere presence of such a notice might be sufficient to justify the assumption that any further attempts to operate or access the contents of the system will be conducted in the knowledge that this is unauthorized. The installation of a security system, typically allocating authorized users with passwords and requiring these to be entered at the stage of initial contact, would undoubtedly reinforce this position.

More difficult situations will arise where the user has limited access rights. Typically this may arise within an employment relationship or where computing facilities are made available to students. Here establishing that the user was aware of the fact that his access rights had been exceeded will require that the limitations be specified unambiguously.

The Law Commission refers to the distinction between conduct which constitutes 'a deliberate act of disobedience, and indeed of defiance of the law' and that which amounts to , "merely carelessness, stupidity or inattention'. Only the former it was recommended, should face prosecution under the Computer Misuse Act.

Unauthorized use by authorized users

A further distinction should also be made at this point. The legislation prohibits unauthorized access. It does not strike at the situation where access is authorized but the, use to which it is put is unauthorized. As the Law Commission point out, the use of an office typewriter to type a private letter will not expose a typist to criminal sanctions and it would be most inequitable to alter that situation merely because a word processor was used:

There may, however, be situations where such an approach may limit the effectiveness of the legislation. In the case of DPP v Bignell a police officer obtained access to data held on the police national computer in order to identify the owner of a motor vehicle. The information

was sought for the owner's personal interest and was not connected with his duties as a police officer. The conduct being discovered he was charged with an offence under Section 1 of the Computer Misuse Act. Although it was not contended that the use to which the data was put was unauthorized, the Divisional Court accepted submissions by counsel for the respondent to the effect that:

> . . . the primary purpose of the Computer Misuse Act was to protect the integrity of computer systems rather that the integrity of information stored on the computers. . . . a person who cause's a computer to perform a function to secure access to information held at a level to which the person was entitled to gain access does not commit an offence under Section 1 even if he intends to secure access for an unauthorized purpose because it is only where the level of unauthorized access has been knowingly and intentionally exceeded that an offence is committed, provided the person knows of that unauthorized level of access.

and held that no offence had been committed under the Computer Misuse Act. It was suggested by the court that an offence may have been committed under the Data Protection Act. An example of this possibility can be taken from a recent Scottish case. Here, the assistance of a police officer was sought by a friend who considered that his daughter had entered into an unsuitable relationship. Upon consulting the police computer, the officer discovered a reference that the man. involved was a hepatitis risk. He subsequently telephoned the woman involved urging her to break off the relationship on the ground that the man was 'riddled with AIDS'.

This conduct was held to constitute an unauthorized disclosure of data and the officer was convicted of a breach of Section 5 of the Data Protection Act and fined £500. Under the provisions of this section, any obtaining, holding, disclosure or international transfer of data by a servant or agent of a data user which contravenes the terms of the latter's entry on the Register will render the individual concerned liable under both criminal and civil law on the same basis as the data user.

In a case such as R v Thompson the appellant was presumably authorized to access the computer, but clearly was not entitled to act in the manner at issue. Assuming that the courts were to endorse the Law Commission's interpretation of the concept of unauthorized access such a person would not be guilty of an offence under Section 1 of the Act. Section 2, the ulterior intent offence discussed below, appears relevant but this can only be committed by a person who has committed the basic unauthorized access offence.

Although, as occurred in Thompson, most instances of computer fraud can be prosecuted under general criminal provision, the effect of this situation might be to deny much on the protection offered by the Computer Misuse Act to employers faced with authorized but dishonest employees.

16.7 The ulterior intent offence

One of the most complex areas of the law is that concerned with the concept of criminal attempts. In most cases, including the offences established under the Computer Misuse Act, the attempt to commit an offence will be considered as serious a matter as its successful completion.

The question arises, however, when an attempt can be considered to have been made. The Criminal Attempts Act, 1981 draws a distinction between conduct which is preparatory to the commission of an offence and that which constitutes part of its perpetration. The dividing line between preparation and perpetration is seldom clear-cut. The Law Commission in its Report identified a number of problems which might arise in the computer field creating circumstances where conduct might not constitute an attempt under the general provisions of criminal law but which was felt to ju5tify special treatment within the computer context.

The first example concerned a hacker who secured access to a bank's computer system, the system being used for electronic fund transfers. In order to accomplish a transfer a password would have to be transmitted. The Law Commission hypothesized that the hacker might attempt to transmit a large number of combinations in the hope of finding the correct one. In the event that the password was discovered, used, and a transfer of funds accomplished, the Law Commission was in no doubt that the offence of theft would be committed.

The act of transmitting combinations of numbers and letters in the attempt to, discover a valid password would not, it considered, be regarded as more than conduct preparatory to the commission of a crime. As such it would not constitute a criminal attempt, especially in the event that further steps would be required in order to complete the transfer. In such a situation, the existence of the ulterior intent offence would serve to bring forward in time the moment at which a serious criminal offence might be committed. A second illustration utilized by the Law Commission concerned a would-be blackmailer who obtained access to

data held on a computer in order to obtain confidential personal information which might be used for the purpose of blackmail.

A more detailed example of this form of behavior was reported during the second reading debate in the House of Commons where it was alleged that the medical records of a patient who was HIV positive were penetrated and the information used for blackmail purposes. Once again, it is unlikely that conduct of that nature could, at the stage of obtaining the data from the computer, constitute a criminal attempt. Reference has previously been made to the speed at which Vast sums of money may be transferred using an electronic fund transfer system. In terms of time, it seems clear that the gap between conduct preparatory to a crime and its perpetration may be very short where this form of conduct is at issue. Assuming the correctness of the Law Commission's expressed view that the conduct in its first example would not suffice to constitute an attempt, there would appear a case for the extension of the criminal law. It might be argued, however, that this should take the form of modifying the law of attempt rather than establishing a new offence. The blackmail example utilized by the Law Commission appears less satisfactory.

Certainly, such conduct is to be regarded as reprehensible, but there appears little difference in principle between a party who secures access to medical data held in paper files and those held on computer. The only justification for the approach adopted might be that in many instances the 'old-fashioned' blackmailer might engage in some form of unauthorized entry to property coupled with theft of documents in order to secure the information. Such conduct will be criminal in its own right and may well attract heavier penalties than those available under the Computer Misuse Act's basic offence.

16.8 The impossible dream

It is immaterial for the purpose of the ulterior intent offence whether the further offence is intended to be committed on the same occasion as the unauthorized access offence or at some future time. It will also constitute no form of defence that the commission of the further offence would prove impossible.

In the banking example cited above, the basis for the ulterior intent offence will be established even though, unbeknown to the perpetrators, further security precautions would render impossible the successful completion of their scheme.

16.9 Application of the ulterior intent offence

The application of the ulterior intent offence was at issue in the case of R v Governor of Brixton Prison, ex p Levin, referred to previously In order for the United States' extradition request to be met, it was necessary to establish that the acts committed by the defendant would have constituted criminal offences under English law. There was no doubt that Levin, in hacking into the Citibank's computer system, had committed the unauthorized access offence. It may be queried how useful a role is played by the ulterior intent offence.

In the Levin case, the extradition request was upheld upon a range of grounds-including breach of the unauthorized modification offence established by Section 3 of the Computer Misuse Act. The finding that the ulterior intent offence had been committed was not critical to the decision. A more significant limitation is created by the requirement that the unauthorized access offence also be committed. This excludes the authorized but dishonest user who, by all accounts, is responsible for most loss and damage in this area.

16.10 Unauthorized modification of data

Given its intangible nature information is not susceptible of being destroyed in any physical sense. A simple example might be a user erasing a piece of music stored on an audio tape. If the original recording was of a chart-topping song, destruction of one copy does not affect the song itself. Equally, the physical elements of the tape suffer no harm.

The tape was and remains a physical item capable of recording and storing certain forms of data. Two consequences may follow from this act. First, assuming that the erasure was carried out erroneously, the owner of the tape may require to expend time and money in securing a further copy. The second consequence may be even more serious. If the tape represented not a copy of a chart-topping song but the only recording of the work in question, a unique item will be lost to the world. If an author types out a chapter of a book on information technology law using a word processor, the contents represent a recording of the author's knowledge of the subject. If the text is erased, and assuming that the author was sufficiently negligent to fail to maintain back-up copies, the knowledge remains but it is most unlikely that the particular recording can ever be reproduced. In the illustration given, the

damage may be principally to the author's peace of mind. In other situations, significant financial loss may arise. If a mail order company's list of customers should be deleted and no replacement be readily available, the ability of the company to continue in business might be imperiled to a considerable extent.

Anyone possessing a degree of familiarity with computers and their method of operation will be only too well aware how fragile is the hold on its electronic life of any piece of data. The accidental depression of a key or the placing of a computer disk in undue proximity to a magnetic field as produced by electrical motors or even telephones, can speedily consign data to electronic oblivion. To the risks of accidental damage have to be added those of deliberate sabotage.

The vulnerability of computer sets to such events is not questioned. Once again, our concern must be with the legal consequences which may follow such behavior. The basic scenario involves a party altering or deleting data held on a computer system, such action taking place without the consent of the system owner. Within this a wide range of activities can be identified. At the most basic level, the perpetrator may use 'delete' or 'reformat' commands or even bring a magnet into close proximity to a computer storage device.

Amendment of data may be made for a variety of motives. In some cases, such as that of Levin discussed above, amendment of data may be a component of a scheme of fraud. Other actions may be driven by the intent to cause disruption to the computer owner's activities. This might involve manipulation of computer programmes through, for example, the insertion of logic bombs, whilst an ever expanding range of computer viruses present a continual threat to the wellbeing of computer owners.

16.11 Logic Bombs

A logic bomb maybe defined as a programme which is designed to come into operation at some later date or upon the occurrence of specified conditions. Two examples cited by the Audit Commission are not untypical of this form of behavior. In the first case, a departing employee inserted a programme into the computer with the intention that it would cause messages to be displayed on the screen whenever his leaving date was entered into the system.

The programme did not operate in the manner intended but proved more harmful, resulting in the unavailability of the system for a period of about two hours. In this case the computer breakdown would appear to have been an unintended consequence of the programme, although the employee involved was successfully prosecuted on a charge of criminal damage. The second illustration is not dissimilar.

Here, prior to leaving his employment, an employee made an alteration to the language preferences of the system software so that error messages would be presented in French, Dutch or German instead of in English. The modification was structured in such a way that it would not take effect until some time after the employee's departure. On this occasion no prosecution was brought, the Audit Commission reporting that the individual was rebuked and agreed to make a contribution towards the cost of correction.

Although the instances reported above might appear lacking in malicious intent, other logic bombs are specifically designed to cause the corruption or erasure of data. An example might be taken from the case of IZ v Thompson discussed above and the appellant's attempt to cause the computer to erase records of his activities.

16.12 Computer Viruses

Perhaps the most notorious form of conduct in the computer field consists of the creation and/or dissemination of computer viruses. In many instances, the effect of a virus will be indistinguishable from that of a logic bomb. The difference between the two concepts is that whilst a logic bomb is normally created on and applied to a particular computer system, a virus will typically be transferred from one system to another. This may occur through the transfer of disks or other storage devices.

Computer viruses can take a wide variety of forms. One of the less harmful examples of the species is the 'Cookie Monster'. Inspired by an American television character, this causes the message I want a cookie' to appear on the computer screen. If the user types the word 'cookie'; the message disappears, otherwise it returns with increasing frequency. In similar vein, the 'ping pong' virus causes the image of a bouncing ball to cross and re-cross the screen. In neither instance are any data or programmes affected.

Other viruses are considerably more malign. One which is reported to have infected computers in a Maltese bank had the effect of corrupting data. Evidencing a somewhat warped sense of humour on the part of its creator, the virus gave the user the opportunity to play what was effectively a game of chance. If the user won, the data would be restored, otherwise it would be permanently erased.

In other cases, not even this degree of opportunity is given to the user to avoid permanent-loss of his data. One of the most notorious examples of a computer virus was the so-called 'AIDS' virus. This was contained on a disk which was mailed to subscribers of a popular computing magazine. Purporting to be an informational programme on the AIDS virus, the programme would corrupt and render useless the data on any computer on which it was loaded. The instance of the AIDS virus raises a number of interesting legal questions.

The disks were accompanied by an instruction leaflet which incorporated a licence agreement. This offered a licence to recipients and gave instructions as to the fees involved and the address (in Panama) to which these should be tendered. The document went on:

> You are advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life . . . and your computer will stop functioning normally

Although the circumstances of the particular case where disks were mailed on an unsolicited basis might elicit little sympathy for the supplier, it may be queried whether the use of a virus as a form of deterrence against illicit copying of software might be considered legitimate in certain situations. In the event, a person allegedly responsible for the promulgation of the AIDS computer virus was arrested in the United States and extradited to stand trial on a charge of demanding money with menaces.

Proceedings were dropped prior to trial in England when the prosecution accepted that the defendant's mental state was such that he was unfit to plead. A final illustration of the destructive power of viruses may be taken from a comment made in the House of Commons during debate on the Computer Misuse Bill. Quoting from a Hong Kong based computer consultant, the view was expressed that: 'Its quite simple. If I wanted my competitor to go bankrupt, I would just anonymously send someone in that company an infected games disk'. In other cases, the dissemination of a virus may not be a part of any scheme of extortion. In

some cases, the virus may produce harmful effects beyond anything intended by its originator.

In one of the major cases brought under the United States Computer Fraud and Abuse Act, a student at Cornell University produced and released a virus programme which had the effect of infecting some 6,000 computers in academic institutions throughout the United States. The student's intention, it would appear, was to demonstrate his programming ability by causing a single copy of the programme to be placed on all these computers. This would have caused no damage or inconvenience but the programme replicated itself over and over again, effectively using up all of the victims' processing capacity and preventing their normal operations.

16.13 The Legal Response

Reference was made in a number of the instances cited by the Audit Commission to the fact that criminal sanctions had been imposed against those held responsible. The application of offences relating to damage to property represented some of the first attempts to apply general legal provisions in the context of computer relatec-1 conduct. At least in terms of reported cases, these prosecutions met with a considerable measure of success. In Scotland, where most offences remain rooted in the common law, the offence of malicious mischief was held applicable in a case where conduct prevented the profitable exploitation of property (in this case a nuclear power station) even though no physical damage was caused. In England, the cases of Cox v Riley and R v Whiteley provided authority for the application of the Criminal Damage Act 1971 to forms of computer related conduct. This statute provides that:

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property . . . shall be guilty of an offence.

The word 'property' is defined in Section 10 as 'property of a tangible nature whether real or personal'.

In Cox v Rile, the appellant was employed to operate a computerized saw. This consisted of a powered saw whose operations could be controlled by the insertion of a printed circuit card containing a number of computer programmes The equipment contained a programme cancellation function The appellant, deliberately and without due cause, caused the

programmes to be erased. Although the saw could also be used under manual control, its practical utility was impaired significantly until the owner could obtain a replacement card. This; it was stated, required the expenditure of time and effort of a more than minimal nature'.

The key question before the court was whether an property had been damaged or destroyed. Counsel for Co argued his conduct had affected only the electronic impulses making up the computer programmes. These could not f within the definition of property. This contention was rejected the Divisional Court which held that the critical factor was that as a result of Cox's conduct, the saw s owner was require to expend time and money in restoring the saw itself to original condition, i.e. as a device which could be used to c wood in accordance with instructions transmitted from computer programme.

The offence of criminal damage was successfully invoked in a small number of subsequent English prosecutions. In : original working paper on computer misuse, the La Commission indicated that it considered the legal position the area, of damage to data to be satisfactory. By the time of t publication of the final report this view had changed. Co. Riley, it was suggested, had not confronted fully the point that the dictionary definition of damage required 'some injury to a thing'. The Law Commission concluded:

> That the practical meaning of 'damage' has caused practical as well as theoretical problems following the decision in Cox v Riley is evidenced by the experience of the police and prosecuting authorities who have informed us. that, although convictions have been obtained in serious cases of unauthorized access to data or programmes, there is recurrent (and understandable) difficulty in explaining to judges, magistrates and juries how the facts fit in with the present law of criminal damage.

Supporting this view, reference was made in the House of Commons to the fact that:

> . . . of 270 cases that have been verified by the Department of Trade and Industry as involving compute misuse over the past five years, only six were brought to court for prosecution and only three of these were successfully prosecuted for fraud. There must be some inadequacy in the law as it stands.

Such comments sit a little uneasily with the findings of the Audit Commission. In its report covering the period 1984-87, a span encompassed within the DTI figures, it found 118 instances of computer fraud and misuse and indicated that prosecutions were initiated in 40

cases. Of these prosecutions 35 were successful, three unsuccessful and two pending at the time of the surveys publication.

16.14 Modification in the Computer Misuse Act

The recommendation of the Law Commission was that the Criminal Damage Act should be amended, effectively to reverse the decision in Cox v Riley by making it clear that damage to programmes or data would not constitute the offence of criminal damage. Parallel to this, a new computer-specific offence should be established.

Acting on this recommendation the computer misuse Act provides that an offence will be committed by a person who, acting with intent, causes an unauthorized modification of the contents of any computer. The new provision is intended to overcome the uncertainty concerning the application of the Criminal Damage Act. To avoid the possibility of overlap between the two statutes it is provided that:

> For the purposes of the Criminal Damage Act, 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

The resurrection of criminal damage?

Ironically, no sooner was the Computer Misuse Act to reach the statute book than a further case, R v Whitely, involving the application of a charge of criminal damage to computer-related behavior was decided by the Court of Appeal. In view of the interpretation of the Criminal Damage Act adopted by the court, it would appear that the attempt to exclude its application in the computer context may not be effective.

Within the United Kingdom, computers operated by most institutions in the field of higher education are linked together in a network known as JANET (Joint Academic Network): Although access to the network is controlled by password, a failure in security at one institution allowed the appellant to obtain access tc its computer network. From there, access could readily be obtained to all the other computers on the network.

Operating under the pseudonym 'The Mad Hacker' the appellant made extensive (and expensive) use of the system. Using his computing skills he was able steadily to extend his

user rights eventually obtaining the status of the controller of particular computers. This allowed him to delete the files 'Accounts Journal' and 'Systems Journal' which would otherwise have recorded details of his activity. After some time, the computer operators became aware of unusual activities on their machines.

Efforts were made to detect the intruder and for some considerable time a game of 'cat and mouse' was played. between the appellant and the operators. On one occasion, the appellant was reported as having been sufficiently 'astute to detect a special programme (sic), inserted by the legitimate operator to trap him and deleted it'. On a further occasion, the appellant succeeded in 'locking' legitimate users out of the computer systems. On occasion, the appellant's activities caused computer systems to 'crash' and increasingly insulting messages were left in files.

Ultimately, British Telecom instituted monitoring of telephone calls into computers favored by the appellant. Detecting a suspicious call, this was traced back to the appellant's home. He was arrested and charges of criminal damage subsequently brought. As with many incidents recounted previously, no damage was caused to any physical components but operations were seriously impaired and considerable staff time was expended in restoring the systems to full operation and in tracking down the perpetrator.

The prosecution's contention, which was accepted both by the jury and the Court of Appeal, was that the changes made to the information held on the system would constitute criminal damage. Delivering the judgment of the court the Chief Justice (Lane) ruled:

What the Act requires to be proved is that tangible property has been damaged, not necessarily that the damage itself is tangible. There can be no doubt that the magnetic particles upon the metal discs were a part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner.

Although the judge went onto refer to the provisions of the Computer Misuse Act and comment that no doubt it will be used as the basis of criminal prosecution in the case of computer misuse the passage cited above would appear to suggest that damage to data held on a computer disk might still be regarded as adversely. affecting its 'physical.condition'. Such a result would have significant consequences, first in that the penalties which might be imposed .under the Criminal Damage Act are more substantial than those applying under the

Computer Misuse Act and, second, that the prosecution in a case brought under the 1971 Act requires to prove only that the accused acted 'recklessly'.

The standard under the Computer Misuse Act is, of course, that the accused acted intentionally. It might also be noted that the 1990 Act makes no change to Scots law,, and indeed the Scottish Law Commission was of the view that existing provisions were adequate as a response to instances of computer misuse, so that existing offences of malicious mischief and vandalism might still be invoked. The issue of the continuing applicability of existing provisions may assume particular significance in one situation. As indicated above, the 1990 Act prohibits unauthorized modification of the 'contents of a computer'. The contents of computer disks or other forms of storage device are protected only when the disks are held in a computer. A scenario can be identified in which two individuals secure unauthorized access to art office containing a computer and a box of computer disks. Both individuals carry a magnet. One uses this to corrupt the contents of the computer's hard disk; the other produces a similar effect on the contents of the box of disks. We can assume further that the box of disks represents a 'back-up copy' of the material held on the computer. In this situation, one person will be guilty of an offence under the Computer Misuse Act and the other will not.

Given the nature and purpose of the legislation, this ma, be a justifiable situation. The question will be whether the second party might be prosecuted under the Criminal damage Act. Certainly there is no doubt that conduct of this kind could, prior to 1990. Although it might be argued that the wording of Section 3(6) excludes the application of the Criminal damage Act only where damage occurs whilst storage devices are held in a computer system, the expository problems identified by the Law Commission would pale into insignificance compared with those of distinguishing damage' to the contents of a disk occurring whilst it is held in a computer and the same damage occurring when it is outside.

16.15 Operation of the unauthorized modification offence

The concept of modification encompasses the addition of data or its alteration or erasure. A modification will be regarded as unauthorized if the person causing it is not authorized so to act or does not possess the consent of a person who is so entitled. Again, the possibility of different categories of rights and privileges attaching to different users must be borne in mind.

Typically, an employee or a student may be entitled to use the facilities of a computer system but will not be entitled to delete any portions or to add any programmes. At the most basic level of activity, it would apply in the situation where a user intentionally causes the deletion of programmes or data held on a computer.

The manner in which this is accomplished will be immaterial. At the simplest Level, the user may operate delete function's so as to remove progranmes or data. In the first prosecution brought under this provision of the Act, the accused had installed a security package on a computer belonging to a firm which he claimed owed some £2,000 in fees. The effect of the installation was to prevent the computer being used unless a password was entered. As this was not disclosed, the computer was effectively rendered unusable for several days with resultant losses estimated at some £36,000.

The accused was convicted and fined £1,60. Amendments to data may also produce adverse effects. In one reported case, a nurse altered prescription details and other records on a hospital computer. The possible consequences of such activities do not need to be described and a conviction was secured under the Act. An offence may also be committed when data is added to a computer system. One instance of this, which will be discussed below, occurs when a computer is infected with a virus.

The offence will also be committed where logic bombs or other programrnes are added to the computer system with the intent that these will operate so as to cause inconvenience to the computer user. In one instance an IT manager added a programme to his employer's system which had the effect of encrypting incoming data. The data would automatically be decrypted when it was subsequently accessed. The manager left his employment following a disagreement and some time later the decryption function. ceased to operate. Once again, the effect was to render the computer unusable. Despite claims that. the encryption function was intended as a security device and that the failure of the decryption facility was an unforeseen error, the manager was convicted of an offence under the Act.

A more interesting case brought under the legislation concerned a contract for the supply of bespoke software. The customer was late in making payment for the software and shortly afterwards the software stopped working. It transpired that the supplier, anticipating possible problems with payment, had inserted a time lock function. Unless removed by the supplier upon receipt of payment the software woulc-1-stop working from a specified date.

This conduct resulted in prosecution and conviction under the unauthorized modification offence.

The issues raised in this case are undoubtedly less clear cut than in a number of the other prosecutions brought under the Act. It was argued that the use of such time-locks was a legitimate response to the failure of the customer to meet its contractual obligation to pay for the software. A further point which does not appear to have been raised was whether the supplier would retain sufficient intellectual property rights in the software to be entitled to control its continued use.

It could also be argued that the action would have been lawful had notice been given to the customer of the fact that the software would stop working if payment was not made timeously. It may be that the drafting of the offence is sufficiently broad to make the mere act of unauthorized use illegal. An example might concern an employee who types private letter using his employer's computer. As Section 2(5 states that the fact whether a modification is permanent o temporary is immaterial, it would not even appear that there is a necessity for the text of the letter to be stored on the computer. In the event that a portion of text is stored on computer's hard disk, utilizing only a minuscule fraction of the disk's storage capacity, any degree of impairment of the computer's capabilities will be similarly minute.

The Act, however, does not require that the degree impairment be substantial or significant. Such conditions would add further levels of complexity and uncertainty to task of defining the scope of the legislation. It is to be recognized however, that the act of making an unauthorized modification constitutes only one element of the offence and that prosecution is required additionally to establish that the p responsible intended to impair the operation of the comp In addition to proscribing acts impairing the operation computer, the unauthorized modification offence may': committed when data held on a computer is modified in a fashion which may affect its reliability.

A possible scenario might involve an individual giving false information with a view to causing the modification unfavorable entry on a credit reference agency's files.

Viruses and the unauthorized modification offence

Taking the concept of an unauthorized modification as a whole it would seem clear that the offence might be committed by a person who creates a computer virus and sends it out into the world with the intention that it will infect other computers.

The originator will cause the modification of any computer which is infected even though they may not be directly responsible for the infection of any particular machine, this being brought about by an unsuspecting (or even reckless) - authorized user. To this extent the phrase 'to cause' must be interpreted in two senses: in respect of the act which causes the effect and also of the act which is proximately responsible for its occurrence. One of the most publicized cases brought under the Computer Misuse Act involved the prosecution of Christopher Pile.

Using the pseudonym 'Black Baron' the accused was reported as having told detectives that 'he had wanted to create a British virus which would match the worst of those from overseas'. A number of viruses were created by Pile and concealed in seemingly innocuous programmes which he published on the Internet from where they would infect any computer onto which they were downloaded.

In the very recent past many of large corporations network were destabilized by the advent of seemingly innocuous I Love You , virus sent as an attachment to e-mail. This was turned out to be work of a juvenile computer hacker from Manila.

16.16 Hackers Sites

The various Hackers sites are: ·Hackers cracker definition

- Hackers
- Hacker's paradise
- Internet underground
- 2600 magazine
- Nerd world: Hackers
- Yahoo-Haker's page

16.17 Safety on the Internet

To present the cyber crime the various safety related issues are available at the following sites

- Child safety on the internet
- Computer Crime Resources
- Cyber Patrol
- Cyber Sitter Product Info
- Keeping Kids safe in cyberspace
- Safe Surf home page
- Safe Surf news back issues
- Safe Surf Inc.
- Street smart on the web
- Surf watch Home page

16.18 Short Summary

- A hack is a quick fix or clever solution to a restriction
- Access is held to be unauthorized when the user is not himself entitled to control access of the kind in question to programme or data and he does not have the consent it access of the kind in question. To programme or data from any person who is so entitled.
- Right of access does not confer any entitled to transfer these on to a third party.
- Section of the computer misuse act doesnot strike at the situation where access is authorized, but the use to which it is put is unauthorized
- Under the computer misuse act the attempt to commit an offence will be considered as serious a matter as its successful completion.

16.19 Brain Storm

- Mention some of the hackers sites?
- Mention some of the web sites where safety related issues are available?
- Mention some of the cyber crimes with illustration
- What is a viruses? Explain
- Explain the E-Mail security destruction
- Explain the concept of access.
- Whether unauthorized use by authorized users is punishable under section 1 of computer misuse act?

Lecture 17

The Information Technology Act

Objectives

In this lecture you will be

- Knowing about Information Technology Act.

Coverage Plan

Lecture 17

17.1 Snap Shot

17.2 The Information Technology Act 2000

17.3 Preliminary

17.4 Definition

17.5 Short Summary

17.6 Brain Storm

17.1 Snap Shot

The union government on l6th December 1999 introduced in the lok sabha the much-awaited cyber law legislation to provide the legal framework for electronic commerce and to enable electronic governance in the country.

The information technology bill 1999 is a bill to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian penal code, 1860, the Indian evidence act, 1872, the banker's book evidence act, 1891 and the reserve bank of India act, 1934, and for matters connected therewith or incidental thereto.

New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Business and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Although people are aware of these advantages they are reluctant to conclude business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements as to writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and documents and records which should bear signatures. The law of evidence is traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper based. Transactions, hence to facilitate e-commerce, the need for lega1 changes have become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

Titled 'Information technology bill, 1999' it also seeks to make consequential amendments in the Indian penal code, 1860 and the Indian evidence act, 1872. The bill, introduced by union minister for information technology, Pramod Mahajan, gives equal legal treatment to users of

electronic communication with other conventional forms. The bill envisages to legalize the electronic signatures on the net which would give sanctity to credit card transactions and boost e-commerce business. The bill will also amend the banking act, the evidence act, the telegraph act, and the company law to bring it in line with the new law. In 1998-99, the e-commerce transactions in the country were to the tune of Rs. 131 crore. In the current fiscal year, such transactions are expected to touch Rs. 450 crore ($100 million) against $43 billion worth transactions in the us in 1998.

The new bill proposes to set up licensing, monitoring and certifying authorities for enactment of cyber laws. The authorities would monitor and oversee issues like jurisdiction, origin, authentication, privacy protection and intellectual property, computer crimes committed via information highways on cyber space. A controller would be appointed to enable the government to monitor and regulate activities like creating web pages, advertisements, bulletin board and most importantly e-commerce originating from the country. A cyber regulations appellate tribunal is also proposed to be set up which will hear appeals against decisions of the adjudicating officers on alleged crimes. Contravention of the cyber regulation would be adjudicated by officers who impose penalty in the nature of compensation to the affected.

The bill proposes to enable government departments and ministries to accept the filing, creation and retention of documents in the form of electronic record. The government departments could be free to specify the format under which these document's would be stored. Thus electronic records could replace the tonnes of papers. It provides for a liability to pay compensation for unauthorized access to computer, its network and data base and also seeks to punish a person who makes misrepresentation or suppress any material fact to the controller of it activities.

The majority of the e-commerce transactions in India is currently limited to business to business activities. This is because the buyer and seller are known to each other and they have faith in each other. This does not apply to business-to-consumer transactions, which is why this activity has still not taken off. Once the bill becomes a law and digital Signatures are legalized the business-to-consumer transactions are expected to boom.

17.2 The Information Technology Act 2000

To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electoral communication, commonly/ referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian panel code:, the Indian evidence act, 1872, the banker's book evidence act, 1891 and the reserve bank of India act, 1934 and for matters corrected therewith or incidental thereto.

Whereas the general assembly of the united nations by resolution a / Res / 51 / 162 dated the 30th January, 1997 has adopted the model law on electronic commerce adopted by the united nations commission on international trade law;

And whereas the said resolution recommends inter alia that all states give favorable consideration to the said model law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper based methods of communication and storage of information;

And whereas it is considered necessary to live effect to the said resolution and to promote efficient delivery of government services by means of reliable electronic records

Be it enacted by parliament in the fiftieth year of the republic of India as follows :

17.3 Preliminary

- Short title, extent; commencement and application.-(1) this act may be called the information technology act 2000.

- It shall extend to the whole of India and, save as otherwise provided in this act, it applies also to any offence or Contravention there under committed outside India by any person.

- It shall come into force on such date as the central government may, by notification, appoint and different dates may be appointed for different provisions of this act and any

reference in any such provision to the commencement of this act shall be construed as a reference to the commencement of that provision.

1. Nothing in this act shall apply to;

   - a negotiable instrument as defined in section 13 of the negotiable instruments act, 1881;
   - a power-of-attorney as defined in section la of the powers-of-attorney act, 1882;
   - a trust as defined in section 3, of the Indian trusts act, 1882;
   - a will as defined in clause (h) of section 2 of the Indian succession act, 1925 including any other testamentary disposition by whatever name called;
   - any contract for the sale or conveyance of immovable property or any interest in such property;
   - any such class of documents or transactions as may be notified by the central government in the official gazette.

17.4 Definition

In this act, unless the context Otherwise requires

- "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
- "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
- "adjudicating officer" means adjudicating officer appointed under subsection (1) of section 46;

- "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

- "appropriate government" means as respects any matter,-

  - enumerated w list ii of the seventh schedule to the constitution;

  - relating to any state law enacted under list iii of the seventh schedule to the constitution the state government and in any other case, the central government

- asymmetric crypto system means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

- "certifying authority" means a person who has been granted a license to issue a digital signature certificate Under section 24;

- "certification practice statement" means a statement issued by a certifying authority to specify the practices that the certifying authority employs in issuing digital signature certificates;

- "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

- "computer network" means the interconnection of one or more computers through-

  - the use of satellite, microwave, terrestrial line or other communication media; and

  - terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

- "computer resource" means computer, computer system, computer network, data, computer database or software;

- "computer system" means a device or collection of devices, including w put and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

- "controller" means the controller of certifying authorities appointed under sub-section (1) of section 17;

- "cyber appellate tribunal" means the cyber regulations appellate tribunal established under sub-section (1) of section 48;

- "data" means a representation of information, knowledge, facts, concepts or instructions which am being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

- "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;.

- "digital signature certificate" means a digital signature certificate issued under sub-section (4) of section 35;

- "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory or similar device

- "electronic gazette" means official gazette published in the electronic form;

- "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

- "function", in relation to a computer, includes logic , control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

- "information" includes data, text, images, sound, codes, computer programmes, software and databases or micro film or computer generated micro film;

- "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

- "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

- "Law" includes any act of parliament or of a state legislature, ordinances promulgated by the president or a governor, as the case may be, regulations made by the president under article 240, bills enacted as president's act under sub-clause (a) of clause (l) of article 357 of the constitution and includes rules regulations, bye-laws and orders issued or made thereunder;

- "license" means a license granted to a certifying authority under section 24;
  - "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary
  - "prescribed" means prescribed by rules made under this act;
  - "private key" means the key of a key pair used to create a digital signature;
  - "public key" means the key of a key pair used to verify a digital signature and listed in the digital signature certificate:
  - "secure system" means computer hardware, software, and procedure that
  - art reasonably secure from intrusion and misuse ,
  - provide a reasonable level of reliability and correct operation;
  - are reasonably suited to performing the intended functions; and
  - Adhere to generally accepted security procedures;

- "security procedure" means the security procedure Prescribed under section 16 by the central government;
- subscriber" means a person in whose name the digital signature certificate is issued;
- "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether -

- the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

- the initial electronic record is retained intact or has Been altered since such electronic record was so affixed with the digital signature

- any reference in this act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

17.5 Short Summary

- Information technology bill 1999 was introduced by union minister for information technology Pramod Mahajan. Gives equal legal treatment to users of electronic communication with other conventional forms.
- Information technology bill 1999 proposes to set up licensing, monitoring and certifying authorities for enactment of cyber laws.
- Computer network means the interconnection of the one or more computers through the use of satellite, microwave, terrestrial line or other communication media and terminals or a complex consisting of two or more inter connected computers whether or not the inter connection is continuously maintained.
- Computer systems means computer, computer system, computer network, data, computer database or software.

17.6 Brain Storm

1. Explain the definitions for

a) a computer

b) a computer network

c) Computer resources

d) Computer system

e) Data

f) Electronic Form

g) Electronic Record

h) Information

i) Intermediary

According to the information technology act 2000.

2. What is a private key? How it differs from public key.

Lecture 18

Digital Signature

Objectives

In this lecture you will be

- Knowing about Authentication of electronic records.
- Knowing about Attribution, acknowledgement and dispatch of electronic records.
- Knowing about Duties of subscribers.
- Knowing about controls of Private key.

Coverage Plan

Lecture 18

18.1 Snap Shot

18.2 Authentication of electronic Records

18.3 Electronic Governance

18.4 Attribution, acknowledgement and dispatch of electronic records

18.5 Acknowledgement of Receipt

18.6 Time and place of dispatch and receipt of electronic Record

18.7 Secures electronic records and secure

18.8 Digital Signature Certificates

18.9 Suspension of digital signature certificate

18.10 Revocation of digital signature certificate

18.11 Notice of suspension of Revocation

18.12 Duties of subscribers

18.13 Control of Private key

18.14 Short Summary

18.15 Brain Storm

18.1 Snap Shot

In the session we discuss about digital signature

18.2 Authentication of electronic records :

- subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

- the authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation-for the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result very time the algorithm is executed with the sane electronic record as its input making it computationally infeasible-

- to derive or reconstruct the original electronic record from the hash result produced by the algorithm

- that two electronic records can produce the same hash result using the algorithm.

- any person by the use of a public key of the subscriber can verify the electronic record.

- the private key and the public key me undue to the subscriber and constitute a functioning key pair.

18.3 Electronic governance

Legal recognition of electronic records : where any law, provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

- rendered or made available in an electronic form; and
- accessible so as to be usable for a subsequent reference.

Legal recognition of digital signatures : where any law provides that information .or any other matter shall be authenticated by affixing the signature or, any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature fixed in such manner as may be prescribed by the central government.

Explanation.-for the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

- Use of electronic records and digital signatures is government and its agencies: (1) where any law provides for

  - the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government In a particular manner:

  - the issue or grant of any license, permit, sanction or approval by whatever called in a particular manner;

  - the receipt or payment of money in a particular manner,

Then, not withstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate government. The appropriate government may, for the purposes of sub-section (1), by rules, prescribe

- the manner and format in which such electronic records shall be filed, created or issued;

- the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

- Retention of electronic records.-(1) where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if
- the information contained therein remains accessible so as to be usable for a subsequent reference;

- the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

- the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

- Publication of rules, regulation, etc., In electronic gazette.-where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the official gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order bye-law, notification or any other matter is published in the official gazette or electronic gazette :

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the official gazette or electronic gazette, the date of publication shall be deemed to be the date of the gazette which was first published in any form.

- Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.-nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any ministry or department of the central government or the state government

confer. Right to or any authority or body established by or under, any law or controlled or funded by the central or state government should accept, issue, create, retain, preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

- Power to make rules by central government in respect of digital signature the central government may, for the purposes of this act, by rules, prescribed
  - the type of digital signature;
  - the manner and format in which the digital signature, shall be affixed;
  - the manner or procedure which facilitates identification of the person affixing the digital signature;
  - control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
  - any other matter which is necessary to give legal effect to digital signatures.

18.4 Attribution, acknowledgement and dispatch of electronic records

- Attribution of electronic records.-an electronic record shall be attributed to the originator
  - if it was sent by the originator himself;
  - by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
  - by an information system programmed by or on behalf of the originator to operate automatically.

18.5 Acknowledgement of receipt

1. where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by

   - any communication by the addressee, automated or otherwise; or

   - any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

2. where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator

3. where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee treat the electronic record as though it has never been sent.

18.6 Time and place of despatch and receipt of electronic record-

1. save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the of dispatch control of the originator,

2. save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:

   a. if the addressee has designated a computer resource for the purpose of receiving electronic records;

- receipt occurs at the time when the electronic record enters the designated computer resource; or

- if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

b. if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee

- Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

- The provision of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

- For the purposes of this section;

  - if the originator or the addressee has more than one ~ place of business, the principal place of business, shall be the place of business;

  - if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

  - "usual place of residence", in relation to a body. Corporate, means the place where it is registered.

18.7 Secure electronic records and secure Digital signatures

Secure electronic record : where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Secure digital signature : if, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

a. Unique to the subscriber affixing it;

b. Capable of identifying such subscriber;

c. created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Security Procedure : the central government shall for the purposes of this act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including.

- The nature of the transaction;
- The level of sophistication of the parties with reference to their technological; capacity
- The volume of similar transactions engaged in by other parties;
- The availability of alternatives offered to but rejected by any party;
- The cost of alternative procedures; and
- The procedures in general use for similar types of transactions or communications.

18.8 Digital signature certificates

Certifying authority to issue digital signature certificate :

Any person may make an application to the certifying authority for the issue of a digital signature certificate in such form as may be prescribed by the central government.

- Every such application shall be accompanied by such fee not exceeding twenty five thousand rupees as may be prescribed by the central government, to be paid to the certifying authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

- Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

- On receipt of an application under sub-section (1), the certifying authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries to it may deem fit, grant the digital signature certificate or for reasons to be recorded in writing, reject the application:
- Provided that no Digital Signature Certificate shall be granted unless the certifying authority is satisfied that

  - the applicant holds the private key corresponding to the public key to be listed in the digital signature certificate

  - the applicant holds a private key, which is capable of creating a digital signature;

  - the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection. Y

Representations upon issuance of digital signature certificate : A certifying authority while issuing a digital signature certificate shall certify that

- it has complied with the provisions of this act and the rules and regulations made thereunder;

- it has published the digital signature certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

- the subscriber holds the private key corresponding to the public key, listed in the digital signature certificate;

- the subscriber's public key and private key constitute.. Functioning key air;

- the information obtained in the digital signature certificate is accurate; and

- it has no knowledge of any material fact, which if it had been included in the digital signature certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

18.9 Suspension of digital signature certificate

- subject to the provisions of sub-section

- the certifying authority which has issued a digital signature certificate may suspend such digital signature certificate on receipt of a request to that effect from-
  - the subscriber listed in the digital signature certificate; or
  - any person duly authorised to act on behalf of that subscriber;
  - if it is of opinion that the digital signature certificate should be suspended in public interest.

- a digital signature certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of, being heard in the matter.

- on suspension of a digital signature certificate under this section, the certifying authority shall communicate the Same to the subscriber.

18.10 Revocation of digital signature certificate

- a certifying authority may revoke a digital signature certificate issued by it

- where the subscriber or any other person authorised by him makes a request to that effect; or
- upon the death of the subscriber; or
- upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

- subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a certifying, authority may revoke a digital signature certificate which has been issued by it at any time, if it is of opinion that
  - a material fact represented in the digital signature. Certificate is false or has been concealed;
  - a requirement for issuance of the digital signature certificate was not satisfied;
  - the certifying authority's private key or security system was compromised in a manner materially affecting die digital signature certificate's reliability;
  - the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, has been it has been dissolved, wound-up or otherwise ceased ' to exist.

- a digital signature certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

- on revocation of a digital signature certificate under this section the certifying authority shall communicate the same to the subscriber.

18.11 Notice of suspension of revocation

- Where a digital signature certificate is suspended or revoked under section 37 or section 38, the certifying authority shall publish a notice of such suspension or revocation, as the case may be in the repository specified in the digital signature certificate for publication of such notice.

- where one or more repositories are specified, the certifying authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

18.12 Duties of subscribers

1. Generating key pair.-where any digital signature certificate, the public key of which corresponds as the private key-of that subscriber which is to be listed in the digital signature certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

2. Acceptance of digital signature certificate.-

- a subscriber shall be deemed to have accepted a digital signature certificate if he publishes or authorities the publication of a digital signature certificate

  - to one or more persons;
  - in a repository, or

Otherwise demonstrates his approval of the digital signature certificate in any manner.

- by accepting a digital signature certificate the subscriber certifies to all who reasonably rely on the information contained in the digital signature certificate that

  - the subscriber holds the private key corresponding to the public key listed in the digital signature certificate and is entitled to hold the same;

  - all representations made by the subscriber to the certifying authority and all material relevant to the information contained in the digital signature

  - Certificate are true;

  - all information in the digital signature certificate that is within the knowledge of the subscriber is true.

18.13 Control of private key

- every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his digital signature certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

- if the private key corresponding to the public key listed in the digital signature certificate has been compromised, then, the subscriber shall communicate the same without any delay to the certifying authority in such manner as may be specified by the regulations.

Explanation.-for the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the certifying authority that the private key has been compromised.

18.14 Short Summary

- Function means an algorithm mapping or translation of one sequence of bits into another.
- Electronics record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro film.

- The electronic record is retained in the format in which it was originally generated, sent, or recorded or in a format which can be demonstrated to represent accurately the information. Originally generated sent or received.

- If the originator fails to stipulate the form method of acknowledgement, any communication by the addressee, automated, or otherwise; or any conduct if the addressee, sufficient to indicate to the originator that the electronic record has been received. Is an acknowledgement.

- If the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.

- A digital signature certificate shall not be revoked unless the subscriber has been given an opportunity of being heard.

18.15 Brain Storm

- Explain the duties of the subscribers digital signature certificate?
- How will you revoke digital signature certificate?
- What are the certification given by a certifying authority while issuing a digital signature certificate?
- What are the attribution of electronic record?
- Explain the acknowledgement of receipt in electronic records?

Lecture 19

Electronic Signatures

Objectives

In this lecture you will be able to

- Know about Retention of electronic records
- Know about effectiveness between parties
- Know about presumption regarding certification

Coverage Plan

Lecture 19

19.1 Snap Shot

19.2 Retention of electronic Records

19.3 Liability of network service providers

19.4 Electronic contracts – Formation and validity

19.5 Effectiveness between parties

19.6 Attribution

19.7 Acknowledgement of receipt

19.8 Time and place of dispatch and receipt

19.9 Secure Electronic Record

19.10 Secure Electronic Signature

19.11 Presumption relating to secure electronic records and signature

19.12 For the purposes of this section

19.13 Secure electronic record with digital signature

19.14 Presumption regarding certificates

19.15 Unreliable digital signature

19.16 Reliance on certificates foreseeable

19.17 Prerequisites to publication of certificate

19.18 Publication for fraudulent purpose

19.19 False or Unauthorized request

19.20 Short Summary

19.21 Brain Storm.

19.1 Snap Shot

Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

19.2 Retention of Electronic Records

Where a rule of law requires that certain documents, records or information by retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied.

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or a in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained and

(d) the consent of the department or ministry of the government organ of state, or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

An obligation to retain documents, records or information in accordance with subsection (1)(c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.

Nothing in this section shall –

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records;

(b) preclude any department or ministry of the government organ of state or a statutory corporation from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department, ministry organ of state or statutory corporation.

19.3 Liability of network service providers

A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third party material in the form of electronic records to which he merely provides access if such liability is founded on

(a) the making, publication, dissemination or distribution of such materials or any statement made in such material or

(b) the infringement of any rights subsisting in or in relation to such material

(2) nothing in the section shall affect

(a) any obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under written law; or

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) for the purposes of this section

"providing access", in relation to third party material, means the provision of the necessary technical means by which third party material may be accessed and includes the automatic and temporary storage of the third party material for the purpose of providing access;

19.4 Electronic Contracts

Formation and validity

1. for the avoidance of doubt, it is hereby declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.
2. Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

19.5 Effectiveness between parties

As between the originator and the address of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

19.6 Attribution

1. an electronic record is that of the originator if it was sent by the originator himself
2. as between the originator and the addressee, and electronic record is deemed to be that of the originator if it was sent
3. by a person who had the authority to act on behalf of the originator in respect of that electronic record ;or
4. by an information system programmed by or on behalf of the originator to operate automatically
5. as between the originator and the addressee, an addressee is entitled to regards an electronic record as being that of the originator and to act on that assumption if-

a. in order to ascertain whether the electronic record was that of the originator, the addressee record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose ; or

b. the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to again access to a method used by the originator to identify electronic records as it own.

Subsection shall not apply

(a) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly

(b) in a case within subsection (3) (b) at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure that the electronic record was not that of the originator; or

(c) if in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic records as that of the originator or to act on that assumption.

Where an electronic records is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

The addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure that the transmission resulted in any error in the electronic record as received.

The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates and other electronic records and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure that the electronic record was a duplicate.

Nothing in this section shall affect the law of agency or the law on the formation of contracts.

19.7 Acknowledgement of receipt

(1) subsection, (2), (3) and (4) shall apply where, on or before sending an electronic record or by means of that electronic record the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or other wise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is treated as through it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified r agreed or, if no time has been specified or agreed within a reasonable time, the originator.

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a) may, upon notice to the addressee, treat the electronic record as though it has never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt it is presumed, un less evidence to the contrary is adduced, that the related electronic record was received by the addressee, but that presumption does not imply that the content of the electronic record corresponds to the content of the record received .

(6) Where the received acknowledge states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed unless evidence to the contrary is adduced, that those requirements have been met.

(7) Except insofar as it relates to the sending or receipt of the electronic record, this part is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt

19.8 Time and place of Despatch and Receipt

Unless otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator.

Unless otherwise agrees between the originator and the addressee, the time of receipt of an electronic record is determined as follows;

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs

i. at time when the electronic record enters the designated information system, at the time when the electronic record is retrieved by the addressee;

ii. if the addressee had not designated an information system, receipt when the electronic record enters an information system of the addressee.

subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under subsection (4)

unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has it place of business.

For the purposes of this section.

If the originator of the addressee has more than one place of business the place of business is that which has the closest relationship to the underlying transaction or, where t here is no underlying transaction, the principal place of business;

If the originator or the addressee does not have a place of business reference is to be made to the usual place of residence and

"Usual place residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

This section shall not apply to such circumstances as the minister may by regulations prescribe.

19.9 Secure Electronic Record

If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification.

For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used including

(a) The nature of the transaction

(b) The sophistication of the parties

(c) The volume of similar transaction engaged in the either or all parties

(d) The availability of alternative offered to but rejected by any party.

(e) The cost of alternative procedure and

(f) The procedures in general use for similar types of transaction.

19.10 Secure electronic signature

If through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved it can be verified that an electronic signature was, at the time it was made

(a) unique to the person using it

(b) capable of identifying such person '

(c) created in a manner or using a means under the sole control of the person using it and

(d) is linked to the electronic records to which it relates in a manner such that if the record was changed the electronic signature should be invalidated, such signature shall be treated as a secure electronic signature

19.11 Presumption relating to secure electronic records and signatures

In any proceedings involving a secure electronic records it shall be presumed unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates

In any proceeding involving a secure electronic signature, it shall be presumed unless evidence to the contrary is adduced, that

The secure electronic signature is t eh signature of the person to whom it correlates and

The secure electronic signature was affixed by that person with the intention of signing or approving the electronic record

In the absence of a secure electronic record or a secure electronic signature, nothing in this part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature

19.12 For the purposes of this section

"secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 16 or 19

"secure electronic signature means an electronic signature treated as a secure electronic by virtue of section 17 to 20

Secure electronic record with digital signature

The portion of an electronic records that is signed with a digital signature shall be traded as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20

For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used including

a. the nature of the transaction
b. the sophistication of the parties
c. the volume of similar transaction engaged in the either or all parties
d. the availability of alternative offered to but rejected by any party.
e. The cost of alternative procedure and

f. The procedures in general use for similar types of transaction.

Effect of Digital Signatures

19.13 Secure electronic record with digital signature

The portion of an electronic records that is signed with a digital signature shall be traded as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20.

Secure digital signature

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate and

(b) the certificate is considered trustworthy in that it is an accurate binding of a public key to a person's identity because

- the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42
- the certificate was issued by a certification authority outside Singapore recognized for this purpose by controller pursuant to regulations made under section 43;
- the certificate was issued by a department or ministry of the government an organ of state or a statutory corporation approved by the minister to act as a certification authority on such condition as he may by regulations impose or specify;
- the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure and the digital signature was properly verified by reference to the sender public key.

19.14 Presumption regarding certificates

It shall be presumed, unless evidence to the contrary is adduced, that the information listed in a certificate issued by a licensed certification issued by a licensed certification authority is correct, except for information identified as subscriber information which has not been verified if the certificate was accepted by the subscriber

19.15 Unreliable digital signature

Unless otherwise provided by law or contract person relying on a digitally signed electronic record assumes the risk that the digital signatures is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors.

- facts which the person relying on the digitally signed electronic record knows or has notice of including all facts listed in the certificate or incorporated in it by reference
- the value or importance of the digitally signed records if known
- the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature and
- usage of trade, particularly trade conducted by trustworthy systems or other electronic means general duties relation to digital signatures

19.16 Reliance on certificates foreseeable

It is foreseeable that person relying on a digital signature will also rely on a valued certificate containing the public key by which the digital signature can be verified

19.17 Prerequisites to publication of certificate

No one may publish a certificate or otherwise make it available to a person known by that person to be in apposition to rely on the certificate or on a digital signature that is verifiable with reference to a public key listed in the certificate, if that person knows that

- the certification authority listed in the certificate has not issued it
- the subscriber listed in the certificate has not accepted it or
- the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature crated prior to such suspension or revocation.

19.18 Publication for fraudulent purpose

Any person who knowingly cerates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offence and shall be liable on conviction to a fine not exceeding 20,000 or to imprisonment for a term not exceeding 2 years or to both.

19.19 False or unauthorized request

Any person who knowingly misrepresents to a certification his identity or authorization for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding 10,000 or to imprisonment for a term not exceeding 6 months or to both.

19.20 Short Summary

- The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption. Expect to the extent that the addressee duplicates and other electronic records and the addressee know should known, had the addressee exercised reasonable care or used any agreed procedure that the electronic record was a duplicate.

- Usual place residence in relating to a body corporate, means the place when it incorporated or otherwise usually consisted.

19.21 Brain Storm

- How to secure digital signature.
- How to secure electronic record.
- How to secure electronic signature.

Lecture 20

Regulation of Certifying Authorities

Objectives

In this lecture you will be able to

- Know about Retention of Foreign Certifying authorities
- Know about various process of certifying authorities

Coverage Plan

Lecture 20

20.1 Snap Shot

20.2 Functions of controller

20.3 Recognition of Foreign Certifying authorities

20.4 Controller to act as a repository

20.5 License to issue digital signature certificates

20.6 Application for License

20.7 Renewal of License

20.8 Rejection of License

20.9 Suspension of License

20.10 Notice of suspension of revocation of License

20.11 Power to Investigate Contraventions

20.12 Access to computers and data

20.13 Display of License

20.14 Surrender of License

20.15 Disclosure

20.16 Secure electronic record with digital certificates

20.17 Secure digital signature

20.18 Presumption regarding signature

20.19 Unreliable digital signature

20.20 Short Summary

20.21 Brain Storm

20.1 Snap Shot

Appointment of controller and other officers the central government may, by notification in the officers :

1. gazette, appoint a controller of certifying authorities for the purposes of this act and may also by the same or subsequent notification appoint such number of deputy controllers and assistant controllers as it deems fit.

2. the controller shall discharge his functions under this act subject to the general control and directions of the central government.

3. the deputy controllers and assistant controllers shall perform the functions assigned to them by the controllers under the general superintendence and control of the controller.

4. the qualifications, experience and terms and conditions of service of controller, deputy controllers and assistant controllers shall be such as may be prescribed by the central government.

5. the head office and branch office of the office of the controller shall be at such places as the central government may specify, and these may be established at such places as the central government may think fit.

6. there shall be a seal of the office of the controller.

20.2 Functions of controller:

The controller may perform all or any of the following functions, namely:

Exercising supervision over the activities of the certifying authorities;

- certifying public keys of the certifying authorities;

- laying down. The standards to be maintained by the certifying authorities;

- Specifying the qualifications and experience which employees of the certifying authorities should possess;

- Specifying the conditions subject to which the certifying authorities shall conduct their business;

- Specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a digital signature certificate and the public key;

- Specifying the form and content of a digital signature certificate and the key;

- Specifying the form and manner in which accounts shall be maintained by the certifying authorities;

- Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

- Facilitating the establishment of any electronic system by a certifying authority either solely or jointly with other certifying authorities and regulation of such systems;

- Specifying the manner in which the certifying. Authorities shall conduct their dealings with the subscribers;

- Resolving any conflict of interests between the certifying authorities and the subscribers;

- Laying down the duties of the certifying authorities;

- Maintaining a data-base containing the disclosure record of every certifying authority containing such particulars as may be specified by regulations, which shall be accessible to public.

20.3 Recognition of foreign certifying authorities

- subject to such conditions and restrictions as may be specified by regulations, the controller may with the previous approval of the central government, and by notification in the official gazette, recognise any certifying authority as a certifying authority for the purposes of this act.

- where any certifying authority is recognised under sub-section (1), the digital signature certificate issued by such! Certifying authority shall be valid for the purposes of this act.

- the controller may if he is satisfied that any certifying authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the official gazette, revoke such recognition.

20.4 Controller to act as repository-

- the controller shall be the repository of all digital signature certificates issued under this act.
- the controller shall
  - make use of hardware, software and procedures that are secure from instruction and misuse
  - observe such other standards as may be prescribed by the central government,
  - To ensure that the secrecy arid security of the digital signatures are assured.

- the controller shall maintain a computerised data-base of all public keys in such a manner that such database and the public keys are available to any member of the public.

20.5 License to Issue Digital Signature Certificates

- Subject to the provisions of sub-section any person may make an application, to the controller, for a license to issue digital signature certificates.

- No licence shall be issued under sub-section (1), unless the applicant fulfills such equipments with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue digital signature certificates as may be prescribed by the central government.

- a license granted under this section shall be valid for such period as may be prescribed-by the `central government;
- not be transferable or heritable, (c) be subject to such terms and conditions as may be specified by the regulation.

20.6 Application for License

- every application for issue of a license-shall be in such form as may be prescribed by the central government.

- every application for issue of a license shall be accompanied by

  - a certification practice statement;
  - a statement including the procedures with respect to identification of the applicant;
  - payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the central government;
  - such other documents, as may be prescribed by the central government.

20.7 Renewal of license:

an application for renewal of a license shall be

- in such form; accompanied by such fees, not exceeding five thousand rupees,

- As may be prescribed by the central government and sh111 be made not less than forty-five days before the date of expiry of the period of validity of the license.

20.8 Procedure for grant or rejection of license the controller may, on receipt of an application under sub-section

- of section grant or 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

- Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

20.9 Suspension of license:

- the controller may, if he is satisfied after making such inquiry, as he may think fit, that a certifying authority has,
  - 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;
  - failed to comply with the terms and conditions subject to which the license was granted;
  - failed to maintain the standards specified under clause (h) of sub-section (2) of section 20;
  - contravened any provisions of this act, rule, regulation or order made thereunder,
  - Revoke the license:
  - Provided that no license shall be revoked unless the certifying authority has been given a reasonable opportunity of showing cause against the proposed revocation.
- the controller may; if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him: Provided that no license shall be suspended for a period exceeding ten days unless the certifying authority has been given a reasonable opportunity of showing cause against the proposed suspension.
- no certifying authority whose license has been suspended shall issue any digital signature certificate during such suspension.

20.10 Notice of suspension of revocation of license

- where the license of the certifying authority is suspended or revoked, the controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him.
- where one or more repositories are specified, the controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

- Provided that the database containing the notice of such suspension or revocation, as the case may be, shall be made available through the web site which shall be accessible round the clock:

- Provided further that the controller may, if he consider necessary, publicize the contents of database in such electronic or other media, as he may consider appropriate.

Power to delegate.-the controller may, in writing, authorise the deputy controller, assistant controller or any officer to exercise any of the powers of the controller under this chapter.

20.11 Power to Investigate Contraventions

- controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this act, rules or regulations made thereunder.

- the controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on income-tax authorities under chapter xiii of the income-tax act 1961 and shall exercise such powers, subject to such limitations laid down under that act.

20.12 Access to computers and data

- without prejudice to the provisions of sub-section (1) of section 68, the controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this act, rules or regulations made thereunder has been committed, have access to any computer system; any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

- for the purposes of sub-section (l), the controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the

computer system, data apparatus or material, to provide him with such reasonable technical' and other assistance as he may consider necessary.

20.13 Certifying authority to follow certain procedures: every certifying authority shall;

- make use of hardware, software, and procedures that are secure from intrusion and misuse;
- provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- adhere to security procedures to ensure that the secrecy and privacy digital signatures are assured; and
- observe such other standards as may be specified by regulations.

Certifying authority to ensure compliance of the act, etc. Every certifying authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement; with the provisions of this act, rules, regulations and orders made thereunder.

Display of license. Every certifying authority shall display its license at a conspicuous place of the premises in which it carries on its business.

20.14 Surrender of License

- Every certifying authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the controller.

- Where any certifying authority fails to surrender a license under sub-section (1), the person in whose favor a license is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

20.15 Disclosure

- every certifying authority shall disclose in the manner specified by regulations
  - its digital signature certificate which contains the public key corresponding to the private key used by that certifying authority to digitally sign another digital signature certificate;
  - any certification practice statement relevant thereto; (c) notice of the revocation or suspension of its certifying authority certificates, if any; and
  - any other fact that materially and adversely affects either the reliability of a digital signature certificate, which that authority has issued, or the authority's ability to perform its services.
- Where in the opinion of the certifying authority, any event has occurred or my situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a digital signature certificate was granted, then, the certifying authority shall
  - use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
  - act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Effect of Digital Signatures

20.16 Secure electronic record with digital signature

The portion of an electronic records that is signed with a digital signature shall be traded as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20

20.17 Secure digital signature

(a) the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate and

(b) the certificate is considered trustworthy in that it is an accurate binding of a public key to a person's identity because

- the certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 42
- the certificate was issued by a certification authority outside Singapore recognized for this purpose by controller pursuant to regulations made under section 43;
- the certificate was issued by a department or ministry of the government an organ of state or a statutory corporation approved by the minister to act as a certification authority on such condition as he may by regulations impose or specify;
- the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure and the digital signature was properly verified by reference to the sender public key.

20.18 Presumption regarding certificates

It shall be presumed, unless evidence to the contrary is adduced, that the information listed in a certificate issued by a licensed certification issued by a licensed certification authority is correct, except for information identified as subscriber information which has not been verified if the certificate was accepted by the subscriber

20.19 Unreliable digital signature

Unless otherwise provided by law or contract person relying on a digitally signed electronic record assumes the risk that the digital signatures is invalid as a signature or authentication of the signed electronic record, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors.

- facts which the person relying on the digitally signed electronic record knows or has notice of including all facts listed in the certificate or incorporated in it by reference
- the value or importance of the digitally signed records if known
- the course of dealing between the person relying on the digitally signed electronic record and the subscriber and any available indicia of reliability or unreliability apart from the digital signature and
- usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

20.20 Short Summary

- The controller shall be the repository of all digital signature certificates issued under this act.
- An application for renewal of a license shall be in such from accompanied by such fees not exceeding five thousand rupees.

20.21 Brain Storm

- How to secure digital signature?
- Why the license is suspended?
- How to apply for license.

Lecture 21

Penalties and Adjudication

Objectives

In this lecture you will be able to

- Know about penalty for damage to computers
- Know about power to adjudicate.

Coverage Plan

Lecture 21

21.1 Snap Shot

21.2 Penalty

21.3 Residuary penalty

21.4 Power to adjudicate

21.5 Short Summary

21.6 Brain Storm

21.1 Snap Shot

In this lecture you are going to learn about. Penalty and its types and reason for getting penalties.

21.2 Penalty

For damage to computer, computer system etc: if any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network;

- Accesses or secures access to such computer computer system or computer network;
- Downloads, copies or extracts any data computer data base or information from such computer system or computer network including information or data held or stored in any removable storage medium;
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- 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;
- Disrupts or causes disruption of any computer, computer system or computer network;
- Denies or causes the denial of access to any person authorised to access any Computer system or computer network by any means;
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this act, rules or regulations made there under;
- Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding ten lakh rupees to the person so affected.

- Explanation: for the purposes of this section;
- "computer contaminant" means any set of computer instructions that are designed
- to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
- by any means to usurp the normal operation of the computer, computer system or computer network;
- "computer database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
- 44. Penalty for failure to furnish information return, etc. - if any person who is required under this actor any rules or regulations made thereunder to -
- furnish any document, return or report to the = is satisfied that the person has committed the contravention, controller or the certifying authority fails to furnish he may impose such penalty or award such compensation as the same, he shall be liable to a penalty not exceeding ~ he thinks fit in accordance with the provisions of that section. One lakh and fifty thousand rupees for each such failure;
- file any return or furnish any information, books or other documents within the time specified there for in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
- Maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

21.3 Residuary Penalty

4vhoever contravenes any rules or regulations made under this act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

21.4 Power to adjudicate

(1) for the purpose of adjudging under this chapter whether any person has committed a contravention of any of the provisions of this act or of any rule, regulation, direction or order made thereunder the central government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a director to the government of India or an equivalent officer of a state government to be an adjudicating officer, for holding an inquiry in the manner prescribed by the central government.

The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of information technology and legal or judicial experience as may be prescribed by the central government.

Where more than one adjudicating officers are appointed, the central government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

1. every adjudicating officer shall have the powers of a civil court which are conferred on the cyber appellate tribunal under sub-section (2) of section 58, and
   - all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and:. 228 of the Indian penal code;

- shall be deemed to be a civil court for the purposes of sections 345 and 346 of the code of criminal Procedure, 1973.

2. Factors to be taken into account by the adjudicating officer.-while adjudging the quantum of compensation under this chapter the adjudicating officer shall have due regard to the following factors, namely

- the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- the amount of loss caused to any person as a result
- Of the default;
- the repetitive nature of the default.

21.5 Short Summary

- Computer virus means nothing but occurrence of corruption in data.
- Residency penalty is not exceeding 25 thousand Rupees.
- Damage means rearranging any Computer resources…
- Without it and Legal or Judicial experience no one shall be appointed as a adjudicating officer.

21.6 Brain Storm

- Write a note on Penalties
- What are the powers given to adjudicate?

Lecture 22

The Cyber Regulations Appellate Tribunal

Objectives

In this lecture you will be able to

- Know about Cyber appellate tribunal
- Know about right to Legal Representation

Coverage Plan

Lecture 22

22.1 Snap Shot

22.2 Establishment of Cyber appellate tribunal

22.3 Term of office

22.4 Appeal to Cyber regulations appellate tribunal

22.5 Procedures and powers of the Cyber appellate tribunal

22.6 Compounding of Contraventions

22.7 Short Summary

22.8 Brain Storm

22.1 Snap Shot

In this lecture you are going to learn about Cyber appellate tribunal and its establishment.

22.2 Establishment of Cyber appellate tribunal

Establishment of cyber appellate tribunal.-(1) the central government shall, by notification, establish one or more appellate tribunals to be known as the cyber regulations appellate tribunal.

the central government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the cyber appellate tribunal may exercise jurisdiction.

Composition of cyber appellate tribunal.-a cyber appellate tribunal shall consist of one person only (hereinafter referred to as the presiding officer of the cyber appellate tribunal) to be appointed, by notification, by the central government.

Qualifications for appointment as presiding officer of the cyber appellate tribunal.-a person shall not be qualified for appointment as the presiding officer of a cyber appellate tribunal unless he

- is, or has been, or is qualified to be, a judge of high court; or
- is or has been a member of the Indian legal service and is holding or has held a post in grade i of that service for at least three years.

22.3 Term of Office

Term of office.-the presiding officer of a cyber appellate tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

Salary, allowances and other terms and conditions of service of presiding officer: the salary and allowances payable to and the other terms and conditions of services including pension, gratuity and other retirement benefits of, the presiding officer of a cyber appellate tribunal shall be such as may be prescribed:
Provided that neither the salary and allowances nor the other terms and conditions of service of the presiding officer shall be varied to his disadvantage after appointment.

Filling up of vacancies.-if, for reason other than temporary absence, any vacancy occurs in the office of the presiding officer of a cyber appellate tribunal, then the central government shall appoint another person in accordance with the provisions of this act to fill the vacancy and the proceedings may be continued before the cyber appellate tribunal from die stage at which the vacancy is filled.

Resignation and removal.-(1) the presiding officer of a cyber appellate tribunal may, by notice in writing under his hand addressed to the central government, resign his office:

Provided that the said presiding officer shall, unless he is permitted by the central government to relinquish his office sooner, continue to hold office until the expiry of three months

- From the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

- The presiding officer of a cyber appellate tribunal shall not be removed from his office except by an order by the central government on the ground of proved misbehaviour or incapacity after an inquiry made by a judge of the supreme court in which the presiding officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

- the central government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid presiding officer.

Orders constituting appellate tribunal to be final and not to invalidate its proceedings.-no order of the central government appointing any person as the presiding officer of a cyber appellate tribunal shall be called in question in any manner and no act or proceeding before a cyber appellate tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a cyber appellate tribunal.

Staff of the cyber appellate tribunal

- The central government shall provide the cyber appellate tribunal with such officers and employees as that government may think fit.

- The officers and employees of the cyber appellate tribunal shall discharge their functions under general superintendence of the presiding officer.

- The salaries and allowances and other conditions of service of the officers and employees of the cyber appellate tribunal shall be such as may be prescribed by the central government.

22.4 Appeal to cyber regulations appellate tribunal:

- Save as provided in sub-section (2), any person aggrieved by an order made by an adjudicating officer under this act may prefer an appeal to a cyber appellate tribunal having jurisdiction in the matter.

- no appeal shall lie to the cyber appellate tribunal from an order made by an adjudicating officer with the consent of the parties.

- every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which, a copy of the order made by the adjudicating officer is received by the person aggrieved an it shall be in such and be accompanied by such fee as may be prescribed:

Provided that the cyber appellate tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

- on receipt of an appeal under sub-section (1), the cyber appellate tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

- the cyber appellate tribunal shall send a copy of every `u order made by it to the parties to the appeal and to the~ concerned adjudicating officer.

- the appeal filed before the cyber appellate tribal under sub-section (1) shall be dealt with by it as expeditiously; possible endeavor shall be made by it to dispose of the app~ finally within six months from the date of receipt of the appeal.

22.5 Procedure and powers of the cyber appellate tribunal

- the cyber appellate tribunal shall not bound by the procedure laid down by the code of civil procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this act and any rules, the cyber appellate tribunal shall have powers regulate its own procedure including the place at which it shall have its sittings.

- the cyber appellate tribunal shall have, for the purposes of discharging their functions under this act, t1 same powers as are vested in a civil court under the code civil procedure, 1908, while trying d suit, in respect of the following matters, namely:
  - summoning and enforcing the attendance of person and examining him on oath;
  - requiring the discovery and production of documents or other electronic records;
  - receiving evidence on affidavits;
  - issuing commissions for the examination of witnesses or documents;
  - reviewing its decisions;
  - Dismissing an application for default or deciding it exparte;
  - Any other matter which may be prescribed.

- every proceeding before the cyber appellate tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian penal code and the cyber appellate tribunal shall be deemed to be a civil court for the purposes of section 195 and chapter xxvi of the code of criminal procedure, 1973.

- Right to legal representation: the appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the cyber appellate tribunal.
- Limitation: the provisions of the limitation act, 1963, shall, as far as may be, apply to an appeal made to the cyber appellate tribunal.

- Civil court not to have jurisdiction: no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this act or the cyber appellate tribunal constituted under this act is empowered by or under this act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this act.

Appeal to high court.-any person aggrieved by any decision or order of the cyber appellate tribunal may file an appeal to the high court within sixty days from the date of communication of the decision or order of the cyber appellate tribunal to him on any question of fact or law arising out of such order:

Provided that the high court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

22.6 Compounding of Contraventions

- any contravention under this chapter may, either before or after the institution of adjudication proceedings, be compounded by the controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, . As the case may be, subject to such conditions as the controller or such other officer or the adjudicating officer may specify:

- Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this act for the contravention so compounded. (2) nothing in sub-section (1) shall apply to a person who Commits the same or similar contravention within a period of three years from the date on which the first contravention, ;. Committed by him, was compounded.

- Explanation-for the purposes of this sub-section, any Second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

- where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall, be taken against the person guilty of such ' contravention in respect of the contravention so compounded. :

Recovery of penalty.-a penalty imposed under this act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the digital signature certificate, as the case may be, shall be suspended till the penalty is paid.

22.7 Short Summary

- A Cyber appellate tribunal shall consist of 1 person only to be appointed by notification by the Central Govt.

- The officers and employees of the Cyber appellate tribunal shall discharge their functions under General Superintendent of the presiding officers.

22.8 Brain Storm

- What are the provisions regarding resignation and removal of the presiding officer of a Cyber appellate tribunal.

- What are the procedures and powers of the Cyber appellate tribunal.

- List out the functions of cyber appellate tribunal.

Lecture 23

Offences

Objectives

In this lecture you will be able to

- Know about Hacking with Computer System.
- Know about Breach of confidentiality and Privacy.

Coverage Plan

Lecture 23

23.1 Snap Shot - Tampering with Source Documents

23.2 Hacking with computer system

23.3 Publishing of information which is obscene in electronic form

23.4 Powers of the Controller to give directions

23.5 Protected system

23.6 Penalty for misrepresentation

23.7 Breach of confidentiality and privacy

23.8 Publications for Fraudulent purpose

23.9 Confiscation

23.10 Short Summary

23.11 Brain Storm

23.1 Snap Shot – Tampering with Source documents

Tampering with computer source documents. whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, .when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

23.2 Hacking with computer system:

- whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

- Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

23.3 Publishing of information which is obscene in electronic form

whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

23.4 Powers of the controller to give directions

- the controller may, by order, direct a certifying authority or any employee of such authority to take such measures or cease carrying. On such activities as specified in

the order if those are necessary to ensure compliance with the provisions of this act, rules or any regulations made thereunder.

- any person who fails to comply with any order tinder sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a ripe not exceeding two lakh rupees or to both.

Directions of controller to a subscriber to extend facilities to decrypt information.-

- if the controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the 10 commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the government to intercept any information transmitted through any computer resource.

- the subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

- the subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

23.5 Protected system

- the appropriate government may, by notification in the official gazette, declare that any Computer, computer system or computer network to be a protected system.

- the appropriate government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub- section (1).
- any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

23.6 Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the controller or the certifying authority for obtaining any license or digital signature certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

23.7 Breach of confidentiality and privacy

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

Penalty for publishing digital signature certificate false in certain particulars

- no person shal1 publish a digital signature certificate or otherwise make it available to ally other person with the knowledge that
  - the certifying authority listed in the certificate has not issued it; or
  - the subscriber listed in the certificate has not accepted it; or
  - the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
- any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

23.8 Publications for Fraudulent purpose

Publications for fraudulent purpose whoever knowingly creates, publishes or otherwise makes available a digital signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Act to apply for offences or contraventions committed outside India

- subject to the provisions of sub-section (2), the provisions of this act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

- the purposes of sub-section (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer; computer system or computer network located in India.

23.9 Confiscation

Confiscation.-any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this act against the person contravening of the provisions of. This act, rules, orders or regulations made thereunder as it may think fit.

Penalties and confiscation not to interfere with other punishments.-no penalty imposed or confiscation made under this act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Power to investigate offences notwithstanding anything contained in the code of criminal procedure, 1973, a police officer not below the rank of deputy superintendent of police shall investigate any offence under this act.

23.10 Short Summary

- Computer source code means the listing of programs, computer command, designs layout and programme analysis of computer resource in any form.
- Penalty for misrepresentation is punishment with imprisonment for a term which may.
- Extend to two years, or with fine which may extend to one lakh rupees or with both.

23.11 Brain Storm

- What are the powers to the controller?
- Explain the rules regarding protected system?

Lecture - 24

Network Service Providers not to be Liable In Certain Cases

Objectives

In this lecture you will be able to

- Knowing about offences by companies
- Knowing about Constitution of Advisory committee

Coverage Plan

Lecture 24

24.1 Snap Shot

24.2 Explanation

24.3 Miscellaneous

24.4 Offences by Companies

24.5 Explanation

24.6 Constitution of Advisory Committee

24.7 Short Summary

24.8 Brain Storm

24.1 Snap Shot

Network service providers not be liable in certain cases.-for the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or 0.that he had exercised all due diligence to prevent the commission of such offence, or contravention.

24.2 Explanation - for the purposes of this section

- "network service provider" means an intermediary;
- "third party information" means any information Dealt with by a network service provider in his capacity as an intermediary.

24.3 Miscellaneous

- Power of police officer and other officers to enter, search, etc.

  - notwithstanding anything contained in the code of criminal procedure. 1973, any police officer, not below the rank of a deputy superintendent of police, or any other officer of the central government or a state government authorized by the central government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this act.

    Explanation.-for the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

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

- the provisions of the code of criminal procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

- Act to have overriding effect: the provisions of this act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

- Controller, deputy controller and assistant controllers to be public servants.-the presiding officer and other officers and employees of a cyber appellate tribunal, the controller, the deputy controller and the assistant controllers shall be deemed to be public servants within the meaning of section 21 of the Indian penal code.

- Power to give directions: the central government may give directions to any state government as to the carrying into execution in the state of any of the provisions of this act or of any rule, regulation. Or order made thereunder.

- Protections of action taken in good faith.-no suit, prosecution or other legal proceeding shall lie against the central government, the state government, the controller or any person acting on behalf of him, the presiding officer, adjudicating officers and the staff of the cyber appellate tribunal for anything which is in good faith done or intended to be done in pursuance of this act or any rule, regulation or order made thereunder.

24.4 Offences by Companies

- where a person committing a contravention of any of the provisions of this act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention w as committed, was in charge of, and was responsible to, the company for the conduct of business of the company as tell as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

24.5 Explanation:-for the purposes of this section;

- "company" means any body corporate and includes a firm or other association of individuals; and

- "director", in relation to a firm, means a partner in the firm.

- Removal of difficulties.

- if any difficulty arises in giving effect to the provisions of this act, the central government may, by order published in the official gazette', make such provisions not inconsistent with the provisions of this act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this act.

- every order made under this section shall be laid, as soon as may be after it is made, before each house of parliament.

- Power of central government to make rules.
  - the central government may, by notification in the official gazette and in the electronic gazette, make rules to carry out the provisions of this act.
  - in particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely

- the manner in which any information or matter may be authenticated by means of digital signature under section 5;
- the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;
- the manner and format in which electronic records shall be filed, created or issued and the method of payment under sub-section (2) of section 6;
- the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;
- the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;
- the qualifications, experience and terms and. Conditions of service of controller, deputy controllers and assistant controllers under section 17;
- other standards to be observed by-the controller under clause (b) of sub-section (2) of section 20;
- the requirements which an applicant must fulfill under sub-section (2) of section 21;
- the period of validity of license granted under clause (a) of sub-section (3) of section 21
- the form in which an application for license may be made under sub-section (1) of section 22
- the amount of fees payable under clause (c) of sub-section (2) of section 22;
- such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;
- the form and the fee for renewal of a license and the fee payable thereof under section 23;
- the amount of late fee payable under the proviso to section 23;
- the form in which application for issue of a digital signature certificate may be made under sub section (1) of section 35;
- The fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub section (2) of Section 35;

- The manner in which the adjudicating officer shall hold inquiry under sub section (1) of section 46
- The qualification and experience which the adjudicating officer shall possess under sub section (2) of section 46
- The salary, allowances and the other terms and conditions of service of the Presiding Officer under sub section (3) of section 54
- The procedure for investigation of misbehaviour or incapacity of the Presiding officer under sub section (3) of section 54
- The salary and allowances and other conditions of service of other officers and employees under sub section (3) of section 56
- The form in which appeal may be filed and the fee thereof under sub section (3) of section 57
- Any other power of a civil court required to be prescribed under clause (g) of sub section (2) of section 58 and
- Any other matter which is required to be pr may be prescribed

Every notification made by the central Government under clause (f) of sub section (4) of section I and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be so however, that any such modifications or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

24.6 Constitution of Advisory committee

- The central Government shall as soon as may be after the commencement of this Act, constitute a committee called the cyber regulations advisory committee

- The Cyber Regulations Advisory Committee shall consist of a chair persona and such number of other official and non official members representing the interests principally affected or having special knowledge of the subject matter as the Central Government may deem fit.

- The cyber Regulations Advisory committee shall advise
  - the central government either generally as regards any rules or for any other purpose connected with this act
  - the controller in framing the regulations under this Act
  - the controller in framing the regulations under this act.
  - there shall be paid to the-non-official members of such committee such traveling and other allowances as the central government may fix.

- Power of controller to make regulations.-the controller may, after consultation with the cyber regulations advisory committee and with the previous approval of the central government, by notification in the official gazette, make regulations consistent with this act and the rules made thereunder to carry out the purposes of this act.

- in particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:
  - the particulars relating to maintenance of data-base containing the disclosure record of every certifying authority under clause (m) of section 18;
  - the conditions and restrictions subject to which the controller may recognise any foreign certifying authority under sub-section (1) of section 19;
  - the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;
  - other standards to be observed by a certifying, authority under clause (d) of section 30;

- the manner in which the certifying authority shall disclose the matters specified in sub-section (1) of section 34;

- the particulars of statement which shall accompany an application under sub-section (3) of section 35. (g) the manner by which the subscriber communicate

- The compromise of private key to the certifying authority under sub-section (2) of section 42.

- every regulation made under this act shall be laid, as soon as may be after it is made, before each house of parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the regulation or both houses agree, that the regulation should not he made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

- Power of state government to make rules.-

  - the state government may, by notification in the official gazette, make power of state rules to carry out the provisions of this act.

  - in particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

    - the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

    - for matters specified in sub-section (2) of section 6; (c) any other matter which is required to be provided by rules by the state government.

- every rule made by the state government under this section shall be laid, as soon as may be after it is made, before each house of the state legislature where it consists of two houses, or where such legislature consists of one house, before that house.

- Amendment of act 45 of' 1860.-the Indian penal code shall be amended in the manner specified in the first Schedule to this act.

- Amendment of act 1 of 1872.-the India n evidence act, 1872 shall be amended in the manner specified in the second schedule to this act.

- Amendment of act 18 of 1891: the bankers' books evidence act, 1891 shall be amended in the manner specified in the third schedule to this. Act.

- Amendment of act 2 of 1934: the reserve bank of India act, 1934 shall be amended in the manner specified in the fourth schedule to this act.

24.7 Short Summary

- Company means any body corporate and includes a firm or other association of Individuals.

- Director in relation to a firm means a partner in the firm.

24.8 Brain Storm

- Write a note on power of police officers and other officers.

- Write a note on power of state government to make rules.

Lecture 25

Electronic Transaction of Singapore

Objectives

In this lecture you will be able to

- Know about Liability of Network service provider.
- Know about Electronic Controls
- Know about secure Electronic Record.

Coverage Plan

Lecture 25

25.1 Snap Shot

25.2 Interpretation

25.3 Purposes and Construction

25.4 Application

25.5 Variation by agreement

25.6 Legal recognition of electronic records

25.7 Requirement For Writing

25.8 Electronic Signatures

25.9 Retention of electronic records

25.10 Liability of Network Service Provides

25.11 Electronic Contracts

25.12 Attribution

25.13 Acknowledgement of receipt

25.14 Time and place of dispatch and receipt

25.15 Secure Electronic Record

25.16 Secure Electronic Signature

25.17 Presumption relating to secure electronic records and Signature

25.18 Secure electronic record with digital signature

25.19 Short Summary

25.20 Brain Storm

25.1 Snap Shot

This act may be cited as the electronic transactions act 1998 and shall come into force on such date as the minister may by notification in the Gazette, appoint.

The minister may appoint different dates for the coming into operation of the different provisions of this act.

25.2 Interpretation

In this act, unless the context otherwise requires

"asymmetric cryptosytem" means a system capable of generating a secure key pair, consisting of private key for creating a digital signature, and a public key to verify the digital signature

"authorised officer" means a person authorised by the controller under section 50;

certificate means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair.

"certification authority" means a person who or an organization that issues a certificate:

"certification practice statement" means a statement issued by a certification authority to specify the practices that the certification authority employs in issuing certificates.

"controller" means the controller of certification authorities appointed under section 41(1) and includes a deputy or an assistant controller of certification authorities appointed under section 41(3);

"correspond", in relation to private or public keys, means to belong to the same key pair;

"digital signature" means an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosytstem of an electronic record using an

asymmetric cryptosystem and a has function such that a person having the initial untransformed record and the signer's public key can accurately determine.

(a) whether the transformation was created using the private key that corresponds to the singer's public key and

(b) whether the initial electronic record has been altered since the transformation was made

"electronic record" means a record generated, communicate, received or stored by electronic, magnetic optical or other means in an information system or for transmission from one information system to another;

"electronic signature" means any letters, characters, number or other symbols in digital form attached to or logically associated with an electronic record and executed or adopted with the intention of authenticating or approving the electronic record.

:hash function means an algorithm mapping or translating one sequence of habits into another, generally smaller set (the has result) such that

(a) a record yields that same hash result every time the algorithm is executed using the same record as input;

(b) it is computationally infeasible that a record can be derived or reconstituted form the hash result produced by the algorithm; and

(c) it is computationally infeasible that a record can be found that produce the same hash result using the algorithm;

"information " includes data, text, images, sound, codes, computer programs software and databases;

"key pair" in an asymmetric cryptosystem, means a private key and its mathematically related public key having the property that the public key can verify a digital signature that the private key create;

"licensed certification authority" means a certification authority licensed by the controller pursuant to regulations made under section 42;

"operational period of a certificate" begins on the date and time the certificate is issued by a certification authority (or on a later date and time if stated in the certificate) and ends on the date and time it expires as stated in the certificate or is earlier revoked or suspended;

:private key" means the key of a key pair used to create a digital signature;
"public key" means the key of a key pair used to create a digital signature;

" record "means information that is inscribed, stored or other wise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form;

"repository " mean a system for storing and retrieving certificates or other information relevant to certificate from a specified time;

" rule of law" includes written law;

" security procedure" means a procedure for the purpose of

(a) verifying that an electronic is that of a specific person ; or

(b) detecting error or alteration in the communication content or storage of an electronic record since a specific point in time,.

Which may require the use of algorithms or cods, identifying words or numbers, encryption, answer back or acknowledgement procedures, or similar security devices;

" signed" or " signature" and its grammatical variations includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record including electronic or digital methods;

"subscriber" means a person who is the subject named or identified in a certified issued to him and who holds a private key that corresponds to a public key listed in that certificate;

"suspend a certificate" means to temporarily suspend the operational period of a certificate from a specified time;

"trustworthy system" means computer hardware software and procedures that

(a) are reasonably secure from intrusion and misuse;

(b) provide a reasonable level of availability reliability and correct operation;

(c) are reasonably suited to performing their intended function; and

(d) adhere to generally accepted security procedures;

" valid certificate" means a certificate that a certification authority has issued and which the subscriber listed in its has accepted.

"verify a digital signature", in relation to a given digital signature, record and public key, means to determine accurately

(a) that the digital signature was created using the private key corresponding to the public key listed in the certificate and

(b) the record has not been altered since its digital signature was created.

25.3 Purposes and construction

This act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes;

(a) to facilitate electronic communications by means of reliable electronic records;

(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional an unintentional alteration of records and fraud in electronic commerce and other electronic transactions

(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records ; and

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce and to foster the development of electronic commerce though the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

25.4 Application

1 part 2 or 4 shall not apply to any rule of law requiring writing or signatures in any of the following matters;

(a) the creation or execution of a will;

(b) negotiable instruments;

(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;

(d) any contract for the sale or other disposition of immovable property, or anyinterestin such property;

(e) the conveyance of immovable property or the transfer of any interest in immovable property;

(f) documents of title.

(2) The minister may be order modify the provisions of subsection (1) by adding, deleting or amending any class of transaction or matters.

25.5 Variation by agreement

As between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision of part II or IV may be varied by agreement.

Electronic records and signature generally

25.6 Legal recognition of electronic records

For the avoidance of doubt, it is hereby declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

25.7 Requirement for writing

Where a rule of law requires information to be written in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be unable for subsequent reference.

25.8 Electronic signatures

Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party.

25.9 Retention of electronic records

Where a rule of law requires that certain documents, records or information by retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied.

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or a in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained and

(d) the consent of the department or ministry of the government organ of state, or the statutory corporation which has supervision over the requirement for the retention of such records has been obtained.

An obligation to retain documents, records or information in accordance with subsection (1)(c) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.

A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.

Nothing in this section shall –

(a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records;

(b) preclude any department or ministry of the government organ of state or a statutory corporation from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department, ministry organ of state or statutory corporation.

25.10 Liability of network service providers

A network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third party material in the form of electronic records to which he merely provides access if such liability is founded on

(a) the making, publication, dissemination or distribution of such materials or any statement made in such material or

(b) the infringement of any rights subsisting in or in relation to such material

(2) nothing in the section shall affect

(a) any obligation founded on contract;

(b) the obligation of a network service provider as such under a licensing or other regulatory regime established under written law; or

(c) any obligation imposed under any written law or by a court to remove, block or deny access to any material.

(3) for the purposes of this section

"providing access", in relation to third party material, means the provision of the necessary technical means by which third party material may be accessed and includes the automatic and temporary storage of the third party material for the purpose of providing access;

25.11 Electronic Contracts

Formation and validity

(1) for the avoidance of doubt, it is hereby declared that in the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.

(2) Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

Effectiveness between parties

As between the originator and the address of an electronic record, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

25.12 Attribution

- an electronic record is that of the originator if it was sent by the originator himself
- as between the originator and the addressee, and electronic record is deemed to be that of the originator if it was sent
- by a person who had the authority to act on behalf of the originator in respect of that electronic record ;or
- by an information system programmed by or on behalf of the originator to operate automatically
- as between the originator and the addressee, an addressee is entitled to regards an electronic record as being that of the originator and to act on that assumption if-

(a) in order to ascertain whether the electronic record was that of the originator, the addressee record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose ; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to again access to a method used by the originator to identify electronic records as it own.

- subsection (3) shall not apply

(a) from the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly

(b) in a case within subsection (3) (b) at any time when the addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure that the electronic record was not that of the originator; or

(c) if in all the circumstances of the case, it is unconscionable for the addressee to regard the electronic records as that of the originator or to act on that assumption.

Where an electronic records is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption then, as between the originator and the addressee, the addressee is entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

The addressee is not so entitled when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure that the transmission resulted in any error in the electronic record as received.

The addressee is entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that the addressee duplicates and other electronic records and the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure that the electronic record was a duplicate.

Nothing in this section shall affect the law of agency or the law on the formation of contracts.

25.13 Acknowledgement of receipt

(1) subsection, (2), (3) and (4) shall apply where, on or before sending an electronic record or by means of that electronic record the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or other wise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(3) where the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is treated as through it has never been sent, until the acknowledgement is received.

(4) where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified r agreed or, if no time has been specified or agreed within a reasonable time, the originator.

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a) may, upon notice to the addressee, treat the electronic record as though it has never been sent, or exercise any other rights it may have.

(5) where the originator receives the addressee's acknowledgement of receipt it is presumed, un less evidence to the contrary is adduced, that the related electronic record was received by the addressee, but that presumption does not imply that the content of the electronic record corresponds to the content of the record received .

(6) where the received acknowledge states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it is presumed unless evidence to the contrary is adduced, that those requirements have been met.

(7) Except insofar as it relates to the sending or receipt of the electronic record, this part is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt

25.14 Time and place of Despatch and Receipt

Unless otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator.

Unless otherwise agrees between the originator and the addressee, the time of receipt of an electronic record is determined as follows;

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs

- at time when the electronic record enters the designated information system, at the time when the electronic record is retrieved by the addressee;
- if the addressee had not designated an information system, receipt when the electronic record enters an information system of the addressee.
- subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under subsection (4)

unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has it place of business.

For the purposes of this section

If the originator of the addressee has more than one place of business the place of business is that which has the closest relationship to the underlying transaction or, where t here is no underlying transaction, the principal place of business;

If the originator or the addressee does not have a place of business reference is to be made to the usual place of residence and

"Usual place residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

This section shall not apply to such circumstances as the minister may by regulations prescribe.

25.15 Secure Electronic Record

If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, such record shall be treated as a secure electronic record from such specified point in time to the time of verification.

For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used including

(a) the nature of the transaction

(b) the sophistication of the parties

(c) the volume of similar transaction engaged in the either or all parties

(d) the availability of alternative offered to but rejected by any party.

(e) The cost of alternative procedure and

(f) The procedures in general use for similar types of transaction.

25.16 Secure electronic signature

If through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved it can be verified that an electronic signature was, at the time it was made

(a) unique to the person using it

(b) capable of identifying such person '

(c) created in a manner or using a means under the sole control of the person using it and

(d) is linked to the electronic records to which it relates in a manner such that if the record was changed the electronic signature should be invalidated, such signature shall be treated as a secure electronic signature

25.17 Presumption relating to secure electronic records and signatures

In any proceedings involving a secure electronic records it shall be presumed unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates

In any proceeding involving a secure electronic signature, it shall be presumed unless evidence to the contrary is adduced, that

The secure electronic signature is t eh signature of the person to whom it correlates and

The secure electronic signature was affixed by that person with the intention of signing or approving the electronic record

In the absence of a secure electronic record or a secure electronic signature, nothing in this part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature

For the purposes of this section

"secure electronic record" means an electronic record treated as a secure electronic record by virtue of section 16 or 19

"secure electronic signature means an electronic signature treated as a secure electronic by virtue of section 17 to 20

25.18 Secure electronic record with digital signature

The portion of an electronic records that is signed with a digital signature shall be traded as a secure electronic record if the digital signature is a secure electronic signature by virtue of section 20

For the purposes of this section and section 17, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used including

- the nature of the transaction
- the sophistication of the parties
- the volume of similar transaction engaged in the either or all parties
- the availability of alternative offered to but rejected by any party.
- The cost of alternative procedure and
- The procedures in general use for similar types of transaction.

25.19 Short Summary

- Information includes data, text, images, codes, computer programs softwares & hardware…
- Public key means the key of a pair used to create a digital signature.
- Suspend a certificate means to temporarily suspend the operational period of a certificate form a specified time.
- Usual place residence in relation to a body corporate means the place where it is in corporated or otherwise legally constituted.

25.20 Brain Storm

- Discuss the liability of Network Service Provider?
- Discuss about electronic contracts.
- Explain about acknowledgement of receipt?

Lecture 26

General Duties Relation to Digital Signatures

Objectives

In this lecture you will be able to

- Know about prerequisites to publication of certificates.
- Know about Duties of Certification of authorities.
- Know about Control of Private Key.

Coverage Plan

Lecture 26

26.1 Snap Shot – Reliance on certificates foreseeable

26.2 Prerequisites to publication of certificate

26.3 Publication for fraudulent purpose

26.4 False or unauthorized request

26.5 Duties of certification authorities

26.6 Duties of subscriber

26.7 Control of Private Key

26.8 Initiating suspension or revocation

26.9 Appointment of controller and other officer

26.10 Regulation of Certification authorities

26.11 Recognition of foreign certification authority

26.12 Government use of electronic records and signature

26.13 Controller may give direction for compliance

26.14 General Penalties

26.15 Power to exempt

26.16 Short Summary

26.17 Brain Storm

26.1 Snap Shot

It is foreseeable that person relying on a digital signature will also rely on a valued certificate containing the public key by which the digital signature can be verified

26.2 Prerequisites to publication of certificate

No one may publish a certificate or otherwise make it available to a person known by that person to be in apposition to rely on the certificate or on a digital signature that is verifiable with reference to a public key listed in the certificate, if that person knows that

(a) the certification authority listed in the certificate has not issued it

(b) the subscriber listed in the certificate has not accepted it or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature crated prior to such suspension or revocation.

26.3 Publication for fraudulent purpose

Any person who knowingly cerates, publishes or otherwise makes available a certificate for any fraudulent or unlawful purpose shall be guilty of an offence and shall be liable on conviction to a fine not exceeding 20,000 or to imprisonment for a term not exceeding 2 years or to both.

26.4 False or unauthorized request

Any person who knowingly misrepresents to a certification his identity or authorization for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding 10,000 or to imprisonment for a term not exceeding 6 months or to both.

26.5 Duties of certification authorities

Trustworthy system

A certification authority must utilize trustworthy system in performing its services

Disclosure

A certification authority shall disclose

(A) its certificate tht contains the public key corresponding to the private key used by that certification authority to digitally sign another certificate (referred to in this section as a certification authority certificate)

(B) any relevant certification practice statement'

(C) notice of the revocation or suspension of its certification authority certificate and

(D) any other fact that materially and adversely affects either the reliability of a certificate that the authority has issued or the authority ability to perform its services

in the event of an occurrence that materially and adversely affects a certification authority's trustworthy system or its certification authority certificate the certification authority shall

(a) use reasonable efforts to notify any person who is known to be or foreseeable will be affected by that occurrence or

(b) act in accordance with procedures governing such an occurrence specified in its certification practice statement

Issuing of certificate

a certification authority may issue a certificate to a prospective subscriber only after the certification authority

(a) has received a request for issuance from the prospective subscriber and
(b) has

(I) if it has a certification practice statements, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the perspective subscriber ;or

(II) in the absence of a certification practice statement complied with the conditions in subsection

in the absence of a certification practice statement, the certification authority shall confirm by itself or though an authorized agent that

(a) the prospective subscriber is the person to be listed in the certificate to be issued

(b) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent to have custody of the subscriber private key and to request issuance of a certificate listing the corresponding public key;

(c) the information in the certificate to be issued is accurate;

(d) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) the prospective subscriber holds a private key capable of creating a digital signature and

(f) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

Representation upon Issuance of Certificate

By issuing a certificate, certification authority represents, to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the=certificate or of which the relying person has notice

In the absence of such certification practice statement, the certification authority represents that it has confirmed that

(a) the certification authority has complied with all applicable requirements of this act in issuing the certificate and if the certification authority has published the certificate or otherwise made it available to such relying person that the subscriber listed in the certificate has accepted it

(b) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate

(c) the subscriber's public key and private key constitute a functioning key pair

(d) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed and

(e) that the certification authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representation in paragraphs

where is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, subsection shall apply to the extent that the representation are not inconsistent with the certification practice statement.

Suspension of certificate

Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a certificate shall a suspend the certificate as soon as possible after receiving a requires by a person whom the certification authority reasonably believes to be

(a) the subscriber listed in the certificate

(b) a person duly authorized to act for that subscriber or

(c) a person acting on behalf of that subscriber, who is unavailable

Revocation of certificate

A certification authority shall revoke a certificate that it issued after

(a) receiving a request for revocation by the subscriber named in the certificate and confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation

(b) receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead or

(c) upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

Revocation without subscriber's consent

A certification authority shall revoke a certificate regard less of wheterh the subscribers listed in the certificate consents, if the certification authority confirms that

(a) a material fact represented in the certificate is false

(b) a requirements for issuance of the certificate was not satisfied

(c) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate reliability

(d) an individual subscriber is dead; or

(e) a subscriber has been dissolved, would up or others wise ceased to exist

upon effecting such a revocation other than under subsection (1) (D) or (e) , the certification authority shall immediately notify the subscriber listed in the revoked certificate

Notice of Suspension

Immediately upon suspension of a certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the certificate for publication of notice of suspension

Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.

Notice or Revocation

Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.

Where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories

26.6 Duties of Subscribers

Generating key pair

If the subscriber generates the key pair whose public key is to be listed in certificate issued by a cortication authority and accepted by the subscriber, the subscriber, shall generate that key pair using a trustworthy system

This section shall not apply to a subscriber who generates the key pair using a system approved by the certification authority.

Obtaining certificate

All material representations made by the subscriber to a certification authority for purposes of obtaining a certificate including all information know to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber knowledge and belief, regardless of whether such representations are confirmed by the certification authority

Acceptance of certificate

A subscriber shall be deemed to have accepted a certificate if he

(a) published or authorizes the publication of a certificatel

(a) to one or more person or

(b) in a repository or

(b) by accepting a certificate issued by himself or a certification authority the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate

(b) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true and

(c) all information in the certificate that is within the knowledge of the subscriber is true.

26.7 Control of Private Key

By accepting a certificate issued by a certification authority the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to person not authorized to create the subscribers digital signature

Such duty shall continue during the operation all period of the certificate and during any period of suspension of the certificate.

26.8 Initiating suspension or revocation

A subscriber who has accepted a certificate shall as soon as possible request the issuing certification authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised

26.9 Appointment of controller and other officers

The minister shall appoint a controller of certification authorities for the propose of this act and, in particular for the purpose of licensing, certifying monitoring and overseeing the activities of certification authorities

The controller may after consultation with the minister appoint such number of deputy and assistant controllers of certification authorities and officers as the controller considers necessary to exercise and perform all or any of the powers and duties of the controller under this act or any regulations made there under.

The controller, the deputy and assistant controllers and officers appointed by the controller under subsection shall exercise discharge and perform the powers, duties and functions conferred on the controller under this act or any regulation made there under subject to such directions as may be issued by the minister.

The controller shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority which shall contain all the particulars required under the regulations made under this act.

In the application of the provisions of this act to certificates issued by the controller and digital signatures verified by reference to those certificates, the controller shall be deemed to be a licensed certification authority.

26.10 Regulation of Certification Authorities

The minister may make regulations for the regulation and licensing of certification authorities and to define when a digital signature qualifies as a secure electronic signature.

Without prejudice to the generality of subsection (1) the minister may make regulation for or with respect to

(a) applications for licenses or renewal of licensees or certification authorities and their authorized representatives and matters incidental thereto;

(b) the activities of certification authorities including the manner, method and place of soliciting business, the conduct of such solicitation and the prohibition of such salutation from members of the public by certification authorities which are not licensed;

(c) the standards to be maintained by certification authorities

(d) prescribing the appropriate standards with respect to the qualifications, experience and training of applications for any license or their employees;

(e) prescribing the conditions for the conduct of business by a certification

(f) providing for the content and distribution of written printed or visual material and advertisements that may be distributed or used by a person in respect of a digital certificate or key;

(g) prescribing the form and content of a digital certificate or key;

(h) prescribing the particulars to be recorded in, or in respect of accounts kept by certification authorities

(i) providing for the appointment and remuneration of an auditor appointed under the regulations and for the costs of an audit carried out under the regulations;

(j) providing for the establishment and regulation of any electronic system by a certification authority whether by itself or in conjunction with other certifications authorities and for the imposition and variation of such requirements, conditions or restriction as the controller may think fit

(k) the manner in which a holder of a license conducts its dealings with its customers, conflicts of interest involving the holder of a license and its customers, and the duties of a holder of a license to its customers with respect to digital certificates

(l) prescribing any forms for the purposes of the regulations; and

(m) prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act or the regulations.

Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties not exceeding a fine of $50,000 or imprisonment for a term not exceeding 12 months or both.

26.11 Recognition of foreign certification authorities

43.- The Minister may by regulations provide that the Controller may recognize certification authorities outside Singapore that satisfy the prescribed requirements for any of the following purposes;

(a) the recommended reliance limit, if any, specified in a certificate issued by the certification authority;
(b) the presumption referred to in sections 20(b) (ii) and 21.

Recommended reliance limit

A licensed certification authority shall, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate.
(2) The licensed certification authority may specify different limits in different certificates as it considers fit.

Liability limits for licensed certification authorities

Unless a licensed certification authority waives the application of this section a licensed certification authority

(a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification authority complied with the requirements of this Act;

(b) shall not be liable in excess or the amount specified in the certificate as its recommended reliance limit for either-

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or

(ii) failure to comply with sections 26 and 30 in issuing the certificate.

Regulation of repositories

The Minister may make regulations for the purpose of ensuring the quality of repositories and the services they provide including provisions for the standards, licensing or accreditation of repositories.

26.12 Government use of Electronic Records and Signatures

Acceptance of electronic filing and issue of documents

1. Any department or ministry of the Government, organ or State or statutory corporation that, pursuant to any written law-

(a) accepts the filing of documents, or requires that documents be created or retained;

(b) issues any permit, licence or approval; or

(c) provides for the method and manner or payment, may, notwithstanding anything to the contrary in such written law-

(i) accept the filing or such documents, or the creation or retention of such documents in the form or electronic records;

(ii) issue such permit, licence or approval in the form of electronic records; or

(iii) make such payment in electronic form.

2. In any case where a department or ministry or the Government, organ of State or statutory corporation decides to perform any of the functions in subsections (1) (i), (ii) or (iii), such agency may specify-

(a) the manner and format in which such electronic records shall be filed, created, retained or issued;

(b) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);

(c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing the document;

(d) control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality or electronic records or payments; and

(e) any other required attributes or electronic records or payments that are currently specified for corresponding paper documents.

3. Nothing in this Act shall by itself compel any department or ministry or the Government, organ or State on statutory corporation to accept or issue any document in the form of electronic records.

Obligation of Confidentiality

Expect for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under this Part, obtained access to any electronic record, book ,register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

Offence by body corporate

Where an offence under this Act or any regulation made thereunder is committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attribute to any act or default on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Authorised officer

The Controller may in writing authorize any officer or employee to exercise any of the powers of the Controller under this Part.

(2) The Controller and any such officer shall be deemed to be a public servant for the purposes of the Penal Code (Cap 224).

(3) In exercising any of the powers of enforcement under this Act, an authorized officer shall on demand produce to the person against whom he is acting the authority issued to him by the Controller.

26.13 Controller may give directions for compliance

The Controller may by notice in writing direct a certification authority or any officer or employee thereof to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure compliance with the provisions of this Act or any regulations made thereunder.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 12 months or to both.

Power to investigate

The Controller or an authorized officer may investigate the activities of a certification authority in relation to its compliance with this Act and any regulations made thereunder.

(2) For the purposes of subsection (1), the Controller may in writing issue an order to a certification authority to further its investigation or to secure compliance with this Act or any regulations made thereunder.

Access to computers and data

The Controller or an authorized officer shall –

(a) be entitled at any time to-

(i) have access to and inspect and check the operation of any computer system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act;

(ii) use or caused to be used any such computer system to search any data contained in or available to such computer system; or

(b) be entitled to require-

(i) the person by whom or on whose behalf the Controller or authorized officer has reasonable cause to suspect the computer is or has been so used; or

(ii) any person having charge or, or otherwise concerned with the operation of, the computer, apparatus or material,

to provide him with such reasonable technical and other assistance as he may require for the purpose or paragraph (a).

(2) Any person who obstructs the lawful exercise of the powers under subsection (1)(a) or who fails to comply with a request under subsection (1)(b) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both.

Obstruction or authorized officer

Any person who obstructs, impedes, assaults or interferes with the Controller or any authorized officer in the performance of his functions under this Act shall be guilty of an offence.

Production of documents, data, etc.

The Controller or an authorized officer shall, for the purposes of the execution of this Act, have power to do all or any of the following;

(a) require the production of records, accounts, data and documents kept by a licensed certification authority and to inspect, examine and copy and or them;

(b) require the production of any identification document from any person in relation to any offence under this Act or any regulations made thereunder; and

(c) make such inquiry as may be necessary to ascertain whether the provisions of this Act or any regulations made there-under have been complied with.

26.14 General penalties

No prosecution in respect of any offence under this Act or any regulations made thereunder for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both.

Sanction of Public prosecutor

No prosecution in respect of any offence under this Act or any regulations made thereunder shall be instituted except by or with the sanction of the Public Prosecutor.

Jurisdiction of Courts

A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and any regulations made thereunder and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act or any regulations made thereunder.

Composition of offences

The Controller may, in his discretion, compound any offence under this Act or any regulations made thereunder which is prescribed as being an offence which may be compounded by collecting from the person reasonably suspected of having committed the offence a sum not exceeding $5,000.

(2) The Minister may make regulations prescribing the offences which may be compounded.

26.15 Power to exempt

The Minister may exempt, subject to such terms and conditions as he thinks fit, any person or class or persons from all or any of the provisions of this Act or any regulations made there under.

Regulations

The Minister may make regulations to prescribe anything which required to be prescribed under this Act and generally for the carrying out or the provisions of this Act.

Saving and transitional

Where a certification authority has been carrying on or operating as a certification authority has been carrying on or operating as a certification authority before the appointed day and it has obtained a license in accordance with the regulations made under section 42 with in 6 months after the appointed day, all certificates issued by such certification authority before the commencement of this act, to the extent that they satisfy the requirement under this act or any regulations made there under, shall be deemed to have been issued under this act by a licensed certification authority and shall have effect accordingly.
In this section "appointed day "means the date of commencement of this act.

Related amendments to interpretation act

The interpretation act (cap 1) is amended

(a) by inserting immediately after the words "gazette published " in the definition of "gazette" in section 2(1) the words "in electronic or other form"

(b) by inserting immediately after subsection (4) of section 2, the following subsection;

Where a gazette is published in more than one form, the date of publication shall be deemed to be the date that gazette is first published in any form and

(c) by inserting, immediately after sub paragraph of paragraph:

(iv) authority to provide for the manner and method in which any document, record, application, permit, approval or license may be submitted issued or served by electronic means, or for the authentication there of;

Related amendment to evidence act

The evidence act is amended by renumbering section 69 as subsection of that section, and by inserting immediately thereafter the following subsection;

This section shall not apply to any electronic record or electronic signature to which the electronic transaction act 1998 applies.

26.16 Short Summary

- A district court or a magistrate's court shall have jurisdiction to hear and determine all offences under the act of "Jurisdiction of Courts".

- If any person who knowingly creates a certificate for any fraudulent purpose. Shall be guilty of an offence.

26.17 Brain Storm

- Write a note on Duties of Subscribers.
- What are the duties of certification of authorities
- What is control of private key.
- Write a note on general penalties.

Lecture 27

US Administration Statement of Commercial Encryption & Cryptography Policy

Objectives

In this lecture you will be able to

- Know about US Cryptography Policy.
- Know about Export Controls.

Coverage Plan

Lecture 27

27.1 Snap Shot

27.2 The measures the administration is Considering include

27.3 US Cryptography Policy

27.4 Key Management and Recovery

27.5 Export Controls

27.6 Cracking Coded Messages

27.7 Short Summary

27.8 Brain Storm

27.1 Snap Shot

The Clinton administration is proposing a framework that will encourage the use of strong encryption in commerce and private communication while protecting the public safety and national security. It would be developed by industry and will be available for both domestic and international use.

The frame work will permit U.S industry to take advantage of advances in technology pioneered in this country and to compete effectively in the rapidly changing international marketplace of communications computer networks and software. Retaining the U.S industry's leadership in the global information technology market is of longstanding importance to the Clinton administration.

The frame work will ensure that everyone who communicates or stores information electronically can protect his or her privacy from prying eyes and ears as well as against theft of, or tampering with their data. The frame work is voluntary any American will remain free to use any encryption system domestically.

The framework is based on a global key management infrastructure that supports digital signatures and confidentiality. Trusted private sector parties will verify digital signature and also will hold spare keys to confidential data. Those keys could be obtained only by persons or entities that have lost the key to their own encrypted data, or by law enforcement officials acting under proper authority. It represents a flexible approach to expanding the use of strong encryption in the private sector.

This framework will encourage commerce both here and abroad. It is similar to the approach other countries are taking and will permit nations to establish an internationally interoperable key management infrastructure with rules for access appropriate to each country needs and consistent with law enforcement agreements. Administration officials are currently working with other nations to develop the frame work for that infrastructure.

In the expectation of industry action to develop this framework internationally, and recognizing that this development will take time, the administration intends to take action in the near term to facilitate the transition to the key management infrastructure.

27.2 The measures the administration is considering include

- Liberalizing export controls for certain commercial encryption products
- developing in cooperation with industry, performance standards for key recovery systems and products that will be eligible for general export licenses, and technical standards for products the governments will purchase.
- launching several key recovery pilot projects in cooperation with industry and involving international participation
- transferring export control jurisdiction over encryption products for commercial user from the department of state to the department of commerce.

Administration officials continue to discuss the details of these actions with experts from the communication equipment computer hardware and software industries, civil liberties groups and other members of the public, to ensure that the final proposal balances industry actions towards the proposed framework short term liberalization initiatives and public safety concerns.

The administration does not support the bills pending in congress that would decontrol the export of commercial encryption products because of their serious negative impact on national security and law enforcement. Immediate export decontrol by the U.S. could also adversely affect the security interest of out trading partners and lead them to control imports of U.S. commercial encryption products

A cabinet committee continues to address the details of this proposal. The committee intends to send detailed recommendation to the president by early September, including any recommendations for legislation and executive order. The committee comprises the secretaries of state, defense commerce and treasury the attorney general the directors of central intelligence and the federal bureau of investigation and senior representatives from the office of the vice president, the office of management and budget, and the national economic council.

27.3 US Cryptography Policy

WE live in an age of electronic information. Information technology is transforming society, creating new businesses, new jobs and new careers. The technology also creatures new

opportunities for crime and new problems in investigating and prosecuting crime. As a result electronic information be it corporate trade secrets, prerelease government crop statistics, or a patient's medical records, must have strong protection form uninvited modifications of disclosure. Cryptography enables that protection.

The united states is the world leader in information technology . US firms continue to dominate the us and global information system market. Retaining this leadership is important to out economic security. The Clinton administration through its national information infrastructure initiative, has long recognized that government has an important role as a facilitator and catalyst for the industry led transformation of the way we use computer and communicates technology to work and live.

In particular, government has a strong interest in promoting the legitimate use of robust encryption to support US international competitiveness, foster, global electronic commerce, prevent computer crime, and ensure that the information super highway is a safe place to conduct one business. At the same time there is a growing recognition, affirmed most recently by the national academy of science that the use of encryption to conceal illegitimate activates poses a problem for society as a whole, not just for law enforcement and national security. In brief criminals can use encryption to frustrate legal wiretaps and render useless search warrants for strode electronic data. We know of no technical solution to the problems that would result form the global proliferation of strong cryptography. The implications of this are no small matter.

Encrypted computer files have hampered the prosecution of child pornographers. Militia groups advise their members to use encryption to hide illicit weapons financial and other criminal activities. Aldrich Ames was instructed by his soviet handlers to encrypt computer files that he passed to the soviets. And international terrorists and drug dealers increasingly use encryption to prevent law enforcement officials from reading their voice and data transmissions. Grave crimes such as plot to shoot down several airliners over Chicago, have been foiled by the use of wiretaps. Had the FBI been unable to read those transmissions, however, a major tragedy might have ensued.

No restrictions apply to the us domestic use of cryptography, and the administration has no plan to seek restrictions. Cryptography has long been controlled for export for national security reason, so as to keep it from getting into the hands of foreign governments. But it has today become a dual use technology, and international businesses want to use the same

security products both domestically and abroad. The administration is thus under strong pressure to provide relief form cryptography export controls.

For our cryptography policy to succeed, it must be aligned with commercial market forces and operate on an international basis. Further, it should preserve and extend the strong position that US industry enjoys in the global information systems marketplace. Accordingly, the US government is working with US industry and our international trading partners on an approach that will protect information used in legitimate activities, assure the continued safety of Americans from enemies both foreign and domestic, and preserve the ability of the US information system industry to compete worldwide.

27.4 Key Management and Recovery

A consensus is emerging around the vision of a global cryptography system that permits the use of any encryption method the user choose, with a stored key to unlock it when necessary. The encryption key would be provided voluntarily by a computer user to a trusted party who holds it for safekeeping.

This is what many people do with their house keys give them to a trusted neighbors who can produce them when something unexpected goes wrong. Businesses should find this attractive because they do not want to lock up information and throw away the key or give an employee not the company control over company information. An individual might also use this service to ensure that she can retrieve information stored years ago. This will require a new infrastructure, consisting of trusted parties who have defined responsibilities to key owners. Under law, these trusted emergency key recovery organizations would also respond in a timely manner to authorized requests from law enforcement official who required the key to decode information lawfully obtained or seized from a subject of investigation or prosecution.

The federal government will user key recovery encryption on its own computers because it makes good management sense. It would be irresponble for agencies to store critical records with out key recovery risking the loss of the information for programmatic use and the inability to investigate and prosecute fraud or misuse of the information.

A number of US and International Companies are working with the US and other government to create a system of trusted parties who are certified to safeguard the keys. In

some cases, organizations might guard their own keys. In other cases, persons will use the key recovery services provided by third parties, one of site of services that will include electronic directories and electronic "notaries" in support of on-line commerce. Persons will be free to choose the type and strength of encryption that provide the degree of security they believe appropriate for their use. Taken together, an overall key management infrastructure is needed to make electronic commerce practical on a global scale.

Some commercial products and services which provide emergency key recovery are already available. Testing and refinement is needed before a widespread, robust infrastructure is put in place. The US government is committed to supporting the development of such a key management infrastructure through pilots and experimental trials. The State Department is expediting the review of several export license applications that test commercial key recovery on an international scale. An interagency working group is identifying several potential governmental uses of commercial cryptography-both internal transactions and in communications with the public –where key recovery can be tested. A plan outlining these government tests will be available in August. The government will be purchasing key recovery products for its own use, and will adopt a Federal standard for evaluating such products to assure agency purchasers that the key recovery features operate properly. The Department of Commerce will be establishing an industry-led advisory committee to make recommendations regarding such a standard this summer.

While we are open to other alternatives, a key recovery system is the only approach we know of that accommodates all public safety interests. And even it is imperfect to run the risk of losing their keys and being unable to recover their encrypted information, Although in some countries
(eg. France) mandatory key escrowing is already in effect, we are pursuing a market-driven approach in part because we hope and believe that key recovery will develop as a cost-effective service in an electronic commerce infrastructure. We are encouraged in this effort by recent discussions we have had at the Organization for Economic Cooperation and Development(OECD) that are leading to international cryptography management principles which support key recovery.

27.5 Export Controls

No matter how successful we are in realizing this vision, American users of computer technology are demanding stronger encryption for international use now. Although we do not control the use of encryption within the US, we do, with some exceptions, limit the export of none crowed mas-market encryption to products using a key of 40 bits. (The length of the encryption key is one way of measuring the strength of an encryption industry asserts that it is losing overseas sales to its European and raphy as a component of its commercial software and hardware information systems market would cause serious economic damage to the US economy, and could reduce the US government's ability to influence the long-term future of global cryptography. It also argues that because customers do not want ot use one product in the US and a different one overseas, export controls are causing US firms to provide an unsatisfactory level of protection to their electronic information, making them vulnerable to industrial espionage by their competitors and foreign governments.

While 40 bit encryption products are still strong enough for many uses, the Administration recognizes that some export liberalization may be useful to build support for a key management regime. Accordingly, we are actively considering measures that would provide limited, temporary relief from cryptographic export controls in exchange for real, measurable, commitments from industry (eg. Investments in products that support key recovery) towards the building of a key management infrastructure. The liberalization proposals under discussion, which would continue the current one time review of products by the National Security Agency, include: permitting products using longer key lengths to be exported to specific industry sectors such as health care or insurance(similar to current policy for the financial sector); allowing export of nonescrowed products to a list of trustworthy firms beyond those sectors, with provisions for monitoring compliance to prevent product diversion to other firms; export of cryptography-ready operating systems; and, most dramatically, the transfer of jurisdiction over commercial encryption products from the State Department's munitions list to the Commerce Department's list o f dual-use technologies. Our goal is to obtain commitments from industry by the fall.

We must, however, be careful in any relaxation of controls. Other government's law enforcement and national security needs to access material encrypted with US products could drive them to erect trade barriers by imposing import controls on strong none crow encryption products. In addition, we do not want to do anything that would damage own national security or public safety by spreading unbreakable encryption, especially given the international nature of terrorism. Even 40 bit encryption, if widespread and not escrowed, defeats law enforcement.

It is for these reasons that we oppose the legislation(S. 1726) introduced in this Congress by Senator Burns and co-sponsored by Senator Lott and former Senator Dole. Although it contains some provisions, such as the transfer of export control jurisdiction for commercial cryptography to the Commerce Department, with which we could agree if constructed with appropriate safeguards, the bill is unbalanced and make no effort to take into account the serious consequences of the proliferation it would permit.

The importance of the US information technology industry, the security stakes, and increasing Congressional interest make it clear that there is an urgent need for clear policy and direction. The Administrations proposed approach is broadly consistent with industry suggestions and conclusions reached by the National Academy of Sciences in its report. The report recognizes the need to address a complex mix of commercial and security issues in a balanced manner. We agree with that need. We also agree with the report's recommendation that export controls on encryption products need to be relaxed but not eliminated and are actively considering ways of providing short-term relief. (We do not agree with the report's recommendation that we eliminate most controls on 56 bit key length products.). Finally, we agree that key escrow is a promising but not fully tested solution and are promoting the kind of testing the report recommends as a way of demonstrating the solution's viability while providing stronger encryption internationally.

We will continue discussion with industry, other members of the private sector, the Congress, and governments at all levels to arrive at a solution that promotes a future of safe computing in a safe society.

27.6 Cracking Coded Messages

We should not understimate how difficult it is to decode encrypted electronic information. One approach advanced in the popular debate is to provide our law enforcement officials with more computing power. At first glance, this suggestion seems promising, because in theory any encrypted messages can be decoded if enough computing cycles are applied. This approach fails for five reasons;

First it relies on mathematical theory, not operational reality. Digital technology reduces voice, faxes, images, and text in any language to indistinguishable 1's and 0's. A great variety of encryption products are alos available. Under ideal conditions-if the type of

communication or file, language, and encryption, algorithm are known with certainty, and a short key is used encrypt the information- a large, specially designed computer could decode a single message relatively quickly. But State, local, and Federal law enforcement officials do not operate in the clean confines of a high-tech computer center. They must first capture the 1's and 0's and discern what kind of encryption they have encountered.

Second, after the decoding problem is isolated, acquiring a machine to decode a message is neither quick, easy, or inexpensive. Commercially available computers can not be used because they will not have sufficient capacity. It would, for example, take years for the computers used to process all social security claims, payments, and earnings years to decode on message using the Data Encryption Standard(DES), a widely used system originally developed by the US government that uses a 56 bit key.

Third, this approach betrays a misunderstanding of how crimes are prevented. Used only in the most critical cases, legally authorized wiretaps provide crucial information just before a crime is to occur. Thus a near real-time ability to decode messages is needed Days or weeks are too long to wait to find out that a terrorist attack is about to happen.

Fourth, this approach fails to acknowledge the volume of messages that could need decoding. Each wiretap results in the collection of thousands of messages relevant to the investigative purpose of the wiretap. Even under the most ideal conditions, had these messages been encrypted, the computing resources required to decrypt them quickly would simply not be available. And this example does not include the additional burden of decrypting, if possible, any digital information such as computer disks that are seized as evidence after a crime has been committed.

Finally, revealing the precise capabilities of law enforcement agencies to decode messages, as would be necessary in order to present the fruits of that work as evidence in court, could provide a tutorial to criminal elements bent on eluding law enforcement.

27.7 Short Summary

- Cryptography enables strong protection form uninvited modifications of disclosure.

- Cryptography has long been controlled for export for national security reason so as to keep it from getting into the hands of foreign governments.

- The encryption key would be provided voluntarily by a computer user to a trusted party who holds it for safe keeping. To avoid the risk of loss of information for programmatic use.

27.8 Brain Storm

- Explain Cryptography policy and how it works in Us.

Manonmaniam Sundaranar University

Centre for Information Technology

Tirunelveli

SYLLABUS for MS(IT&EC) / MIT

2.5 IT and Cyber Laws

LECTURE 1 Birth of Information Era - Characteristics of Information Society -Development of Computers & Generation - Computers and Law Today - Importance of Internet - Cyberspace & its birth - Legal implications of Cyberspace - The development of the Internet.

LECTURE 2 Information Legal Practices - International Scenario United Kingdom (U.K) - The committee on data protection - The European Union.

LECTURE 3 Theft of Information - The basis of the offence of theft - Property rights in information - Borrowing as theft - Dishonest exploitation of confidential information - Information theft in Japan.

LECTURE 4 Scope of Data Protection - Manual Records and Data Protection - Concepts of Processing - Personal Data - Distinguishing Opinions from Intentions - Computer bureau/processors - Exceptions to the legislation - National security and data protection - Compliance with council of Europe convention - Breaches of Security of Protection

LECTURE 5 Data Protection Principles - Acquisition of Data - Parties authorised to supply - Relevancy and scale of Information obtained - The community charge - Rhondda Borough Council - Exceptions to the fair obtaining requirements - Data Protections and the Media - Fair Processing - Credit Scoring - Caller identification - Processing of Statistical Data - Accuracy and Timorousness of Data - Data Security - Legal Requirements or Advice -Disclosure to the data subjects etc - Preventing Injury - The Exceptions in Perspective - Data Matching - Codes of Practice - Codes under the Directive.

LECTURE 6 Data Protection - Transborder Transnational Data Flows (TBDFS) - National controls over Transborder data flows - Establishing conformity with the conventions requirements -Transfer to another convention state - Transfer to nonsignatory state - Transborder data flows and the directive.

LECTURE 7 Information Technology Copyright - Provider liability for user Misuse - Newsgroup postings and copyright - Copyright and WWW pages - Significant legal Issues - Cable programmes and the WWW - Copyright in headlines -Copyright law in Canada.

LECTURE 8 Nature of Copyright Protection - Right to copyright owner - Substantial Similarity - Literal and non-literal copying - Justifiable similarities - Unconscious Copying - Willful Ignorance - Fair Dealing - Error correction - Back up copies - Reverse Engineering and de-compilation - Reverse Engineering and computer programmers - Other Infringing Acts - Issue of copies to the public - Public Performance -Adaptation

and translation - Moral Rights - Resale and rental of copies of a protected work - Computer programmes as audio or visual works - Digital sampling - Computer programmes as photographs or films - IRP in software: An Indian Perspective - How to be copyright protected - Legal action.

LECTURE 9 Surveillance Through Information Technology - Privacy and Surveillance - Forms of Surveillance - The Impact of Technology - Surveillance in the 1990s - Consequences of Data Surveillance - The Legal Response to Data Surveillance.

LECTURE 10 Individual Rights and Remedies - Implementing Subject Access - Enforced Subject Access - Access Procedures - Providing Access - Examination mark - The extend of access - Data relating to children - Persons suffering mental disorder - Exceptions to the right of access - Law enforcement and taxation - Health Data - Social work data - Judicial appointments.

LECTURE 11 Legal Privilege - Regulation of financial services - Credit Reference Agencies - Information otherwise available to the public - Order of secretary of state - Failure to provide access - Matters arising subsequent to access - Rectification of inaccurate data - Compensation for inaccuracy - Compensation for unauthorized disclosure - Complaints to the registrar - Subject access in perspective.

LECTURE 12 Introduction to E-Commerce Law - Meaning of Electronic Commerce - Business to Business E-commerce - Business to customer E-commerce - Benefits of E-Commerce - Risk of E-commerce - Cyber Laws - Initiatives in India - Electronic commerce and the World Trade Organisation (WTO) - The Opportunities of Company Secretaries - The Challenges of the Information Era Digitalization - Communication -Disaggregating - Impact on Business.

LECTURE 13 Trade Marks and Service Marks - Patient - Trade Secrets - Cyber Space and Cyber Laws - Issues and Recent Trends in Cyber Laws - The role of ICSI - Emergence of Global E-commerce - Types of E-Commerce - Issues - Cyber Laws - The Electronic Commerce Transaction - Creating a Binding Commitment - Functional Equivalence.

LECTURE 14 Sources of Law - Validity and Enforceability of Agreements - Offer and Acceptance - Consideration - Statutes of Frauds - Performance - Compliance - Breach - Enforcement - Liability and damages - Evidence - Notice and conspicuousness - Consumer issues - Personal Jurisdiction - Negotiability - Intellectual Property - Illegal bargains and Criminal Law - Dealing with Legal Uncertainties - Legislation and regulation

LECTURE 15 UN Model Law on Electronic Commerce - Electronic Funds Transfer Act and Regulation - Digital Signature Legislation - Guidelines - Forms of Agreements - Trading Partner Agreements - Value-Added Network Agreements - Interconnection Agreements - Payments Agreements - Security provision in model agreements - Business Model - The Formalistic Model - The Risk-based Model - Analysis of the Models - Business controls in a Digital Environment - Legal Issues: Indian scenario - Policy Guidelines - Conclusion - Digital Signature - Recent Laws on E-commerce in U.K - Dotcoms, get the Legal Thing Right or Legit to the Court - Business Model - Legal Minefields for Dotcoms.

LECTURE 16 Introduction to Cyber Crime and the Law - The Legal response to Computer hacking - The Computer Misuse Act - The Concept of Access - Limits of authority - Knowledge that access is unauthorized - The ulterior intent offence - The impossible dream - Application of the Ulterior Intent Offence - Unauthorized Modification of data - Logic Bombs - Computer Viruses - The Legal Response - Modification in the Computer Misuse Act - Operation of the Unauthorized modification offence - Hackers sites -Safety on the internet.

LECTURE 17 The Information Technology Act - The Information Technology Act 2000 - Preliminary - Definition.

LECTURE 18 Digital Signature - Authentication of Electronic Records - Electronic Governance - Attribution, acknowledgement and dispatch of electronic records - Acknowledgement of Receipt - Time and place of dispatch and receipt of electronic records - Secures Electronic records and secure Digital signatures - Digital Signature Certificates - Suspension of digital signature certificate - Revocation of digital signature certificate - Notice of suspension of Revocation - Duties of subscribers - Control of Private Key.

LECTURE 19 Electronic Signatures - Retention of Electronic Records - Liability of network service providers - Liability of network service providers - Electronic contracts Effectiveness between parties - Attribution - Acknowledgement of receipt - Time and place of dispatch and receipt - Secure Electronic Record - Secure Electronic Signature - Presumption relating to secure electronic records and signature - For the purpose of this section - Effect of Digital Signatures - Presumption regarding certificates - Unreliable digital signature - Reliance on certificates foreseeable - Prerequisites to publication of certificates - Publication for fraudulent purpose - False or Unauthorized request

LECTURE 20 Electronic Signatures - Functions of controller - Recognition of foreign Certifying authorities - Controller to act as a repository - License to issue digital signature certificates - Application for License - Renewal of License- Rejection of License - Suspension of License - Notice of suspension of revocation of License - Power to Investigate Contravention - Access to computers and data - Display of License - Surrender of License - Disclosure - Secure Electronic record with digital certificates - Secure Digital certificate - Presumption regarding certificates - Unreliable digital signature.

LECTURE 21 Penalties and Adjudication - Penalty - Residuary Penalty - Power to Adjudicate

LECTURE 22 The Cyber Regulations Appellate Tribunal - Establishment of Cyber appellate tribunal - Term of office - Appeal to Cyber regulations appellate tribunal - Procedures and powers of the Cyber appellate tribunal - Compounding of Contravention

LECTURE 23 Offences - Tampering with Source Document - Hacking with computer system - Publishing of information which is obscene in Electronic forms - Powers of the controller to give directories - Protected system - Penalty for misrepresentative - Breach of confidentially and privacy - Publications for Fraudulent purpose - Confiscation

LECTURE 24 Network Service Providers not to be Liable In Certain Cases - Explanation of the section - Miscellaneous - Offences by Companies - Explanation for the offences by companies- Constitution of Advisory Committees

LECTURE 25 Electronic Transaction of Singapore - Interpretation - Purposes and Construction - Application - Variation by agreement - Legal recognition of electronic records - Requirement for Writing - Electronic Signatures - Retention of electronic records - Liability of Network Service Provides - Electronic Contracts - Attribution - Acknowledgement of receipt -Time and place of dispatch and receipt - Secure Electronic Record - Secure Electronic Signature - Presumption relating to secure Electronic records and signature - Secure Electronic Record with Digital Signature

LECTURE 26 General Duties Relation to Digital Signatures - Reliance on Certificate Foreseeable - Prerequisites to publication of certificate - Publication for fraudulent purpose - False or unauthorized request - Duties of certification authorities - Trustworthy system - Disclosure - Issuing of Certificate - Representation upon Issuance of Certificate – us pension of certificate - Revocation of certificate- Notice of suspension - Notice of Revocation- Duties of subscriber - Generating -Key pair - Obtaining certificate- Acceptance of certificate- Control of Private Key - Initiating suspension or revocation - Appointment of controller and other officer - Regulation of Certification authorities - Recognition of foreign certification authority - Recommended reliance limit - Liability limits for licensed certification authorities - Regulation of repositories - Government use of electronic records and signature - Acceptance of electronic filing and issue of documents - Obligation of Confidentiality- Offence by body corporate- Authorised officer- Controller may give direction for compliance - Power to investigate- Access to computers and data- Obstruction or authorized officer - Production of documents, data etc- General Penalties - Sanction of Public prosecutor- Jurisdiction of Courts- Composition of offences- Power to exempt - Regulations - Saving and transitionals -Related amendments to interpretation act- Related amendment to evidence act.

LECTURE 27 US Administration Statement of Commercial Encryption & Cryptography Policy - The measures the Administration is Considering include - US Cryptography Policy - Key Management and Recovery - Export Controls - Cracking Coded Messages.

Best of Luck