UNIT- 10

ISSUES OF SECURITY; ISSUES OF PRIVACY; TECHNICAL ISSUES IN CYBER CONTRACT

STRUCTURE

10.1 INTRODUCTION

Data on our own personal computers can compromise us in unpleasant ways, with consequences ranging from personal embarrassment to financial loss. Transmission of data over the Internet and mobile networks is equally fraught with the risk of interception, both lawful and unlawful- which could compromise our privacy. In this age of cloud computing when much of "our" data- our emails, chat logs, personal profiles, bank statements, etc. reside on distant servers of the companies whose services we use. Our privacy becomes only as strong as these companies' internal electronic security systems. Internet has spawned new kinds of annoyances from electronic voyeurism to spam or offensive email to 'phishing'- impersonating someone else's identity for financial gain, each of which have the effect of impinging on one's privacy.

In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.

10.2 OBJECTIVES

After reading this unit you will be able to understand the following:

- Security issues in cyber contract
- Privacy issues in cyber contract
- Phishing
- Liability for body-corporates
- Technical issues in cyber contract

10.3 SUBJECT

10.3.1 ISSUES OF SECURITY

In electronic commerce the issue of security and a statutory monitoring agency become crucial factors and the same will become crucial aspects of electronic contracts for the consumers to protect their interests and for the business establishments to conduct their business without costly legal battles. The essential security aspects of e-commerce, which need to be taken care in contracts, are:

a. Entity authentication (identifying with whom you are transacting)

b. Message integrity
c. Payment non-repudiation
d. Effective audit
e. Privacy

Such security requirements should also be affordable and the process requires uniform platforms in terms of scalability and transaction models backed by technology. These issues are crucial in drawing up the contracts, which are not part of the physical transaction contracts existing hitherto. As E-commerce means global business in volume and transactions anywhere at any time with customers not known prior to transactions, it is crucial these aspects are taken care. The current Information Technology Act, 2000 provides for the security aspects through sections 14, 15 and 16.

10.3.1.1 RELEVANT PROVISIONS OF INFORMATION TECHNOLOGY ACT, 2000

Section 14. -Secure electronic records. -

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.

Section 15. -Secure digital signature. -

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

(a) Unique to the subscriber affixing it;

(b) Capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Section 16. -Security procedure. -

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

Apart from these issues, the Act enables for a certifying authority and officers and functions in section 17 and they're of from section 18 to 34 on the various aspects of security and privacy issues.

Section 17. -Appointment of Controller and other officers. -

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent

notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
(6) There shall be a seal of the Office of the Controller

10.3.2 ISSUES OF PRIVACY

In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.
Contracts drawn in cyber world need to take care of the mutual interest of the establishments and the clients. This needs an adequate legal framework and the section 35- 39 of Information Technology Act, 2000 deals on the digital signature and its various aspects which will be dealt in length in module 3 on e-banking. However the Act also specifies duties of subscribers which is of importance in contracts drawn from the point of the establishments under Chapter VIII.

10.3.2.1 DUTIES OF SUBSCRIBERS

Section 40. Generating key pair-
Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.
Section 41.Acceptance of Digital Signature Certificate-
(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he Publishes or authorises the publication of a Digital Signature Certificate
(a) to one or more persons;
(c) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that-
(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(b) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Section 42. Control of private key-

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and takes all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation. -

For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromise.

10.3.5 VIOLATION OF PRIVACY IS A MAJOR THREAT UNDER SECURITY ISSUE

According to Information technology Act, 2000, "computer resource" means computer, computer system, computer network, data, computer data base or software; this definition is wide enough to cover most intrusions which involve any electronic communication devices or networks — including mobile networks. Intrusions into computers and mobile devices includes the following:

- accessing[1]
- downloading/copying/extraction of data or extracts any data
- introduction of computer contaminant[2];or computer virus[3]
    - causing damage either to the computer resource or data residing on it
- disruption
- denial of access
- facilitating access by an unauthorized person

---

[1]Under section 2(1)(a) of the IT Act, 2000, "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;

[2]Section 43 of the IT Act, 2000 defines "computer contaminant" as any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

[3]"computer virus" has been defined in section 43 of the IT Act, 2000, as “any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

- charging the services availed of by a person to the account of another person,
- destruction or diminishing of value of information
- stealing, concealing, destroying or altering source code with an intention

The Act provides for the civil remedy of "damages by way of compensation" for damages caused by any of these actions. In addition anyone who "dishonestly" and "fraudulently" does any of these specified acts is liable to be punished with imprisonment for a term of upto three years or with a fine which may extend to five lakh rupees, or with both.

10.3.3.1 PHISHING – OR IDENTITY THEFT

The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else's login credentials to gain access to protected systems, or by the unauthorized application of someone else's digital signature in the course of electronic contracts. Increasingly a new type of crime has emerged wherein sim cards of mobile phones have been 'cloned' enabling miscreants to make calls on others' accounts. This is also a form of identity theft.

Two sections of the amended IT Act penalize these crimes:

Section 66C[4] makes it an offence to "fraudulently or dishonestly" make use of the electronic signature, password or other unique identification feature of any person. Similarly, section 66D makes it an offence to "cheat by personation"[5] by means of any 'communication device'[6] or 'computer resource'.

Both offences are punishable with imprisonment of up to three years or with a fine of up to Rs. one lakh.

10.3.3.2 LIABILITY FOR BODY-CORPORATES

The newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing

[4]"Whoever fraudulently or dishonestly make use of electronic signature or password or any other unique identity feature of any person shall be punished with imprisonment of either description for a term which may extended to three years and shall also be liable to fine which may extended to rupees one lakh."

[5]"Cheating by personation" is a crime defined under section 416 the Indian Penal Code. According to that section, "a person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is." The explanation to the section adds that "the offence is committed whether the individual personated is a real or imaginary person". Two illustrations to the section further elaborate its meaning: (a) A cheats by pretending to be a certain rich banker of the same name. A cheats by personation (b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

[6]Communication device" has been defined to mean "cell phones, personal digital assistance (sic) or combination of both or any other device used to communicate send or transmit any text, video, audio or image".

which they would be liable to compensate those affected by any negligence attributable to this failure.

It is only the narrowly-defined 'body corporates'[7] engaged in 'commercial or professional activities' who are the targets of this section. Thus government agencies and non-profit organizations are entirely excluded from the ambit of this section. This does not necessarily mean that these entitles are exempt from taking reasonable care to safeguard information that they collect, maintain or control – only that remedies against the government must be sought under general common law, rather than under the IT Act.[8]

"Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to.

The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government.

By defining both "sensitive personal data" and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.

In February 2011, the Ministry of Information and Technology, published draft rules under section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold.

10.3.3.3 SENSITIVE PERSONAL INFORMATION

Rule 3 of these Draft Rules designates the following types of information as 'sensitive personal information':

- password;
- user details as provided at the time of registration or thereafter;
- information related to financial information such as Bank account/credit card/debit card/other payment instrument details of the users;
- physiological and mental health condition;
- medical records and history;(vi) Biometric information;
- information received by body corporate for processing, stored or processed under lawful contract or otherwise;

[7]Section 43A defines "'body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
[8] http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- call data records;

This however, does not apply to "any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005".

They and "any person" holding sensitive personal information are forbidden from "keeping that information for longer than is required for the purposes for which the information may lawfully be used". This is perhaps ambiguous, since the potential 'lawful uses' are numerous and could be inexhaustible. It is unclear whether "lawful usage" is coterminous with "the uses which are disclosed to the individual at the time of collection". In addition, this rule is framed rather weakly since it does not impose a positive obligation (although this is implied) to destroy information that is no longer required or in use.[9]

10.3.3.4 MANDATORY PRIVACY POLICIES FOR BODY CORPORATES

Rule 4 of the draft rules enjoins a body corporate or its representative who "collects, receives, possess, stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information". Here "Provider of data" is not the same as individuals to whom the data pertains, and could possibly include intermediaries who have custody over the data.

The policy must provide details of:

- Type of personal or sensitive information collected under sub-rule (ii) of rule 3;
- Purpose, means and modes of usage of such information;
- Disclosure of information as provided in rule 6.

10.3.3.5 PRIOR CONSENT AND USE LIMITATION DURING DATA COLLECTION

In addition to the restrictions on collecting sensitive personal information, body corporate must obtain prior consent from the "provider of information" regarding "purpose, means and modes of use of the information". The body corporate is required to "take such steps as are, in the circumstances, reasonable"[10] to ensure that the individual from whom data is collected is aware of:

- the fact that the information is being collected; and
- the purpose for which the information is being collected; and

[9]http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[10]One wonders about the convoluted language used here when a simpler phrase like "take reasonable steps" alone might have sufficed - reasonableness has generally been interpreted by courts contextually. As the Supreme Court has remarked, "`Reasonable' means prima facie in law reasonable in regard to those circumstances of which the actor, called upon to act reasonably, knows or ought to know. See Gujarat Water Supply and Sewage Board v. Unique Erectors (Guj) AIR 1989 SC 973. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- the intended recipients of the information; and
- the name and address of :
- the agency that is collecting the information; and
- the agency that will hold the information.

During data collection, body corporates are required to give individuals the option to opt-in or opt-out from data collection[11]. They must also permit individuals to review and modify the information they provide "wherever necessary"[12]. Information collected is to be kept securely[13], used only for the stated purpose[14] and any grievances must be addressed by the body corporate "in a time bound manner"[15].

Unlike "sensitive personal information" there is no obligation to retain information only for as long as is it is required for the purpose collected.

The draft rules require a body corporate to obtain prior permission from the provider of such information obtained either "under lawful contract or otherwise" before information is disclosed[16]. The body corporate or any person on its behalf shall not publish the sensitive personal information[17]. Any third party receiving this information is prohibited from disclosing it further[18]. However, a proviso to this sub-rule mandates information to be provided to 'government agencies' for the purposes of "verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences". In such cases, the government agency is required to send a written request to the body corporate possessing the sensitive information, stating clearly the purpose of seeking such information. The government agency is also required to "state that the information thus obtained will not be published or shared with any other person"[19].

---

[11]Sub-Rule 5(7).

[12] Sub-Rule 5(6). It is unclear what would count as a 'necessary' circumstance and who would be the authority to determine such necessity.

[13]Sub-Rule 5(8).

[14]Sub-Rule 5(5).

[15]Sub-Rule 5(9).

[16]Sub-Rule 6(1). There are two problems with this rule. First, it requires prior permission only from the provider of information, and not the individual to whom the data pertains. In effect this whittles down the agency of the individual in being able to control the manner in which information pertaining to her is used. Second, it is not clear whether this information includes "sensitive personal information". The proviso to this rule includes the phrase "sensitive information", which would suggest that such information would be included. This makes it even more important that the rule require that prior permission be obtained from the individual to whom the data pertains and not merely from the provider of information. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[17]Sub-Rule 6(3).

[18]Sub-Rule 6(4).

[19]This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agencies that betrays this statement? Why not instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)? As available at, http://cis-india.org/internet governance/blog/privacy/safeguards-for-electronic-privacy

Sub-rule (2) of rule 6 requires "any information" to be "disclosed to any third party by an order under the law for the time being in force." This is to be done "without prejudice" to the obligations of the body corporate to obtain prior permission from the providers of information[20].

10.3.3.6 REASONABLE SECURITY PRACTICES

Rule 7 of the draft rules stipulates that a body corporate shall be deemed to have complied with reasonable security practices if it has implemented security practices and standards which require:

- a comprehensive documented information security program; and
- Information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

In case of an information security breach, such body corporate will be "required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security program and information security policies".

The rule stipulates that by adopting the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements", a body corporate will be deemed to have complied with reasonable security practices and procedures.

The rule also permits "industry associations or industry clusters" who are following standards other than IS/ISO/IEC 27001 but which nevertheless correspond to the requirements of sub-rule 7(1), to obtain approval for these codes from the government. Once this approval has been sought and obtained, the observance of these standards by a body corporate would deem them to have complied with the reasonable security practice requirements of section 43A.

10.3.3.7 CIVIL LIABILITY FOR CORPORATES

As mentioned above, anybody corporates who fail to observe data protection norms may be liable to pay compensation if:

- it is negligent in implementing and maintaining reasonable security practices, and thereby
    - causes wrongful loss or wrongful gain to any person;[21]

[20]This sub-rule does not distinguish between orders issued by a court and those issued by an administrative/quasi-judicial body. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[21]"Wrongful loss" and "wrongful gain" have been defined by Section 23 of the Indian Penal Code. Accordingly, "Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled. "Wrongful

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act. Further, details of the powers and functions of this officer are given in succeeding sections of this note.

10.3.3.8 CRIMINAL LIABILITY FOR DISCLOSURE OF INFORMATION OBTAINED IN THE COURSE OF EXERCISING POWERS UNDER THE IT ACT

Section 72 of the Information Technology Act imposes a penalty on "any person" who, having secured access to any electronic record, correspondence, information, document or other material using powers conferred by the Act or rules, discloses such information without the consent of the person concerned. Such unauthorized disclosure is punishable "with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

10.3.3.9 CRIMINAL LIABILITY FOR UNAUTHORIZED DISCLOSURE OF INFORMATION BY ANY PERSON OF INFORMATION OBTAINED UNDER CONTRACT

Section 72A of the IT Act imposes a penalty on any person[22] (including an intermediary) who,

- has obtained personal information while providing services under a lawful contract and
- discloses the personal information without consent of the person,
- with the intent to cause, or knowing it is likely to cause wrongful gain or wrongful loss[23]

---

loss"- "Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled." The section also includes this interesting explanation "Gaining wrongfully, losing wrongfully- A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property as well as when such person is wrongfully deprived of property". Following this, it could be possible to argue that the retention of data beyond the period of its use would amount to a "wrongful gain". As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[22] Section 3(39) of the General Clauses Act defines a person to include "any company or association or body of individuals whether incorporated or not". An interesting question here would be whether the State can be considered "a person" so that it can be held liable for unauthorized disclosure of personal information. In an early case of Shiv Prasad v. Punjab State AIR 1957 Punj 150, the Punjab High Court had excluded this possibility. However, the case law on this point has not been consistent. In Ramanlal Maheshwari v.Municipal Committee, the MP High Court held that the Municipal Council could be treated as a 'person' for the purpose of levying a fine attached to a criminal offence. Statutory corporate bodies (such as the proposed UID Authority of India) have been held to be 'persons' for purposes of law . See Commissioners, Port of Calcutta v. General Trading Corporation, AIR 1964 Cal 290. Here under the Calcutta Port Act, Port Commissioners were declared to be a "body corporate", and hence were held to be a 'person'. As available at, http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

[23]See supra n. 44.

Such unauthorized disclosure to a third person is punishable with imprisonment upto three years or with fine upto Rs. five lakh, or both.

10.3.4 TECHNICAL ISSUES

In cyber contract technical issues are:

- Interoperability
- Security
- Privacy
- Connectivity to existing systems (backward compatibility)
  – Web-based front-end systems must be able to connect with back-end legacy systems that tend to be large, complex, and poorly documented.
  – Must use "middleware" to translate data from one system to another

- Internet "pipeline" capacity to support efficient transmission of possibly large-sized contents (music, videos, high-resolution graphics/photos) E.g., Napster phenomenon
  - Web organization – how to conveniently locate product

10.3.4.1 INTEROPERABILITY

Interoperability is the ability of systems running in different operating environments to communicate and work together. – E.g., clients running Windows XP can access Web pages from servers running Linux.
For the interoperability to work, the same set of rules (protocols) must be followed.
Internetworking standard, i.e., TCP/IP– TCP is managing overall network transport function. It breaks the information into data packets, tagging each packet with a sequence number before submitting it to the IP layer. At the other end, TCP layer assembles all packets received and rearrange them in original order. IP is managing addressing and routing. Addressing- determining the addresses to be used and routing – determining the best possible route for packet transmission.

10.3.4.2 SECURITY

Security involves threats to systems. Three types of security threats are:– denial of service, unauthorized access, and theft and fraud. Security.
Denial of Service (DOS)- Two primary types of DOS attacks are spamming and viruses. **Spamming** is sending unsolicited commercial emails to individuals. Also called E-mail bombing, caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Smurfing involves hackers placing software agents onto a third party system and setting it off to send requests to an intended target. DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. **Viruses** are self-replicating computer programs designed to perform unwanted events. **Worms** are special viruses that spread using direct Internet connections. **Trojan Horses** are disguised as legitimate software and trick users into running the program.
Unauthorized access is illegal access to systems, applications or data. Passive unauthorized access is listening to communications channel for finding secrets. Which May use content for

damaging purposes. Active unauthorized access involves modifying system or data including, message stream modification, changes intent of messages, e.g. to abort or delay a negotiation on a contract. Unauthorized access also includes **masquerading** or **spoofing** means sending a message that appears to be from someone else. In other words, impersonating another user at the "name" (changing the "From" field) or IP levels (changing the source and/or destination IP address of packets in the network).**Sniffers** are software that illegally access data traversing across the network. It is the software and operating systems' security hole.

Theft and fraud involves, data theft which is already discussed under the unauthorized access section. Fraud occurs when the stolen data is used or modified. Theft may be of software via illegal copying from company's servers and of hardware, specifically laptops.

10.3.4.3 PRIVACY

Privacy involves threats to data, in which faster and easier data collection through online technology. Cross-referencing (aggregation) may be real offline consumer data with online purchasing habits collected with or without their knowledge. Or cross-referencing online data with other online data between several Web entrepreneurs, for example, hidden data collection without consumer consent, possibly through cookies, e.g. **Usage tracking**– Patterns of online activity lead to inferences about the user's product preferences for providing customized pop-up ads and referring sites. Which may include today's spyware.

Spyware is a type of program that watches what users do with their computer and then sends that information over the Internet to the spyware's author.

10.3.5 TECHNICAL ISSUE INVOLVES IN CONCLUDING THE CYBER CONTRACT

A contract can contain these three distinct types of terms:

- Express terms
- Terms incorporated by reference
- Implied terms

Before a contract can be formally concluded all the terms of the contract must be brought to the attention of the parties. Otherwise, there cannot be a meeting of minds. This is crucial in terms of both e-mail and click wrap contracts. In the former, parties must take care to avoid contradiction and confusion if negotiations of terms are held using e-mail; this is especially so if the negotiations are lengthy. Parties must also take care to identify the documents which are intended to form part of the contract. In the event that terms of a contract are imprecise, the effect of the contract may be substantially altered through a different interpretation of the terms of the terms from that originally intended. In the case of click wrap contracts, web site designers must take care to ensure that all terms are brought to the attention of the consumers before they are presented with the opportunity to purchase a product. Often the terms of click wrap contracts are incorporated by reference. Hence the design of the web site must be such that before the consumer has the opportunity to click 'Submit' or "I Agree', the terms must be clearly brought to his or her attention. The onus is upon the web designers to ensure that

consumers read and acknowledge the terms and conditions. In order to do this effectively, the usual practise has been to require consumers to tick a box or clicks on the acknowledgement that the terms and conditions have been read. If the consumer checks the box or clicks on the acknowledgement, the terms will be incorporated, regardless of whether they have been actually been read. If this is not done, the purchase order or other agreement will not proceed.

Implied terms usually arise separately from the contract formation process and are usually localised. This means that, in the event of a dispute, the governing law of the contract would be a central concern, as would be the type of contract at issue. So this becomes removed from the method of contract formulation in general. Terms may be implied by fact, on the basis of customs or usage, or by construction of the contract. Questions of implied terms are case-specific and will turn on the particular relevant laws of a particular jurisdiction, such as unconscionable conduct or business efficacy or on the subject matter of the contract.

The final step to understand e-contracting is the issue of when and where the contract is formally made or concluded. The general rule is that contract is made when acceptance is communicated from the offeree to the proposer/offeror. Accordingly, there is no contract where the acceptance is not communicated to the proposer, the reason being that it would be unfair to hold proposer by an acceptance of which he has no knowledge. The location of the formation is decided according to where the offeror receives notification of the acceptance. The conclusion of distance contracts has been one of the controversial issues in the law of contract formation. It raises some question marks, especially with regard to the type of rules that should govern the timing of contract formation. It has been argued that the postal acceptance rule applies to the Internet because the communication has been entrusted to a third party such as ISP acting as a parallel to postal system. Also the reason for the application of postal acceptance rule is the system of Internet, similar to postal delivery and hence is non-instantaneous form of communication. The uncertainty regarding the moment of contract formation does not happen in the environment of face-to-face communication or even in distance contracting where an instantaneous method of communication is used. In this kind of contracting, all parties are aware of contract conclusion and they do not face problematic issues such as delay or failure of transmission which occur in non-instantaneous communications. For example, if the offeror asks for notification, then the offeree would need notification of the receipt and so on. Another way of illustrating this is demonstrated if we consider that A is required to receive B's acceptance, then B should have the right to receive notification from A, that the acceptance was received, and A should have the right to receive notification from B, that the notification of receipt of the acceptance was received and so forth. Carrying this on to its logical conclusion, putting the risk in the hands of the offeror would appear logical since it is he who is the master of the offer and he is the position to for or stipulate a specific action in order to be exposed to the potential risk. [vii]In fact, applying the postal rule will avoid such uncertainty and create a definite time regarding to email contract conclusion. Email is considered to be a non-instantaneous method of communication and therefore subject to delay. Contracting by email has been considered as the digital equivalent of the postal system. According to the difficulties with the transmission of email, delays, failure of networks, hacking by third parties or incorrect email addresses of intended recipients, may delay or prevent the delivery of an email. They

suggest therefore, that risk of non-delivery of the email, as with the ordinary post, should lie with the offeror. Nevertheless, it should be kept in mind that similar issues of delay identified in relation to telexes are similarly applicable to email. In fact, no universal rule can cover all situations. These possibilities were not sufficient to persuade courts to find that the general rule of communication should be displaced. Likewise with email, the mere possibility of delays, incorrect addresses or technological failures may not be sufficient to create a universal rule that an email acceptance is effective at a time other than communication. The Supreme Court of India, in ***Bhagwandas Goverdhandas Kedia v Girdharilal Purshottamdas***[x] has held that in case of oral communication or by telephone or telex, an acceptance is communicated when it is actually received by the proposer. When postal rule is applied to e-mail technical consideration come to the fore. The fact remains that e-mail is not instantaneous, the packets may not all arrive there may be congestion on the networks, some of the servers may malfunction and so on. E-mail is also fragmented when compared to a telephone call and the sender has no way of knowing whether the receiver will actually get the message.

In relation to click wrap a different method is involved. The communication between the web client and the server is instantaneous. If the communication between the parties is broken for whatever reasons, the other party will be immediately notified. This is due to the built in self-checking mechanism known as 'checksum'. Therefore, when dealing with click wrap contracts, the postal rule is not applicable as compared to e-mail contracting because the line of communication in click wrap is continually verified, which implies that a communication once sent will be instantly received.

10.4 SUMMARY

In electronic commerce the issue of security and a statutory monitoring agency become crucial factors and the same will become crucial aspects of electronic contracts for the consumers to protect their interests and for the business establishments to conduct their business without costly legal battles. As E-commerce means global business in volume and transactions anywhere at any time with customers not known prior to transactions, it is crucial these aspects are taken care. The current Information Technology Act, 2000 provides for the security aspects through sections 14, 15 and 16. In Internet transactions, e-commerce to succeed the issue of privacy plays a crucial role. Apart from consumer transaction in terms of personal data, the application of internet in banking, privacy is very crucial if not maintained can lead to major financial loss and there of huge litigation costs both to establishments as well as the clients. Hence privacy plays strategic as well as other non-monetary aspects of business in e-commerce.

Contracts drawn in cyber world need to take care of the mutual interest of the establishments and the clients. This needs an adequate legal framework and the section 35- 39 of Information Technology Act, 2000 deals on the digital signature and its various aspects which will be dealt in length in module 3 on e-banking. However the Act also specifies duties of subscribers which is of importance in contracts drawn from the point of the establishments under Chapter VIII the newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive

personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

In cyber contract technical issues are:

- Interoperability
- Security
- Privacy
- Connectivity to existing systems (backward compatibility)
  – Web-based front-end systems must be able to connect with back-end legacy systems that tend to be large, complex, and poorly documented.
  - Must use "middleware" to translate data from one system to another
- Internet "pipeline" capacity to support efficient transmission of possibly large-sized contents (music, videos, high-resolution graphics/photos) E.g., Napster phenomenon
- Web organization – how to conveniently locate product Technical Issues:

A contract can contain these three distinct types of terms:

- Express terms
- Terms incorporated by reference
- Implied terms

Parties must also take care to identify the documents which are intended to form part of the contract. In the event that terms of a contract are imprecise, the effect of the contract may be substantially altered through a different interpretation of the terms of the terms from that originally intended. Implied terms usually arise separately from the contract formation process and are usually localised. This means that, in the event of a dispute, the governing law of the contract would be a central concern, as would be the type of contract at issue. Questions of implied terms are case-specific and will turn on the particular relevant laws of a particular jurisdiction, such as unconscionable conduct or business efficacy or on the subject matter of the contract.

Contracting by email has been considered as the digital equivalent of the postal system. According to the difficulties with the transmission of email, delays, failure of networks, hacking by third parties or incorrect email addresses of intended recipients, may delay or prevent the delivery of an email. In relation to click wrap a different method is involved. The communication between the web client and the server is instantaneous. If the communication between the parties is broken for whatever reasons, the other party will be immediately notified. Therefore, when dealing with click wrap contracts, the postal rule is not applicable as compared to e-mail contracting because the line of communication in click wrap is continually verified, which implies that a communication once sent will be instantly received.

10.5 GLOSSARY

1. IP- Internet Protocol

2. SMURFING- A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. The exploit of smurfing, as it has come to be known, takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). The ICMP is used by network nodes and their administrators to exchange information about the state of the network.

10.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) The essential security aspects of e-commerce, which need to be taken care in contracts, are:
(a) Entity authentication (identifying with whom you are transacting)
(b) Message integrity
(c) Payment non-repudiation
(d) Effective audit
(e) All of above
(ii) According to Information technology Act, 2000, "computer resource" means, (a) computer
(b) computer system
(c) computer network data
(d) computer data base
(e) computer software
(f) All of above
(iii) A computer virus is,
(a) type of virus
(b) type of germs
(c) type of decease
(d) type of self-replicating computer program that causes harm to computer files

(iv) 'Phishing' is also a form of identity theft.

(a) true

(b) false

(v)‘Sensitive personal information’ includes physiological and mental health condition.

(a) true

(b) false

(vi)In cyber contract technical issues are:
(a) Interoperability
(b) Security
(c) Privacy
(d) All of above

(vii) Interoperability is the ability of systems running in different operating environments to communicate and work together.

(a) True

(b) False

(viii)Spamming is also called E-mail bombing.

(a) True

(b) False

(ix) Worms in computer terms is

(a) An insect

(b) A virus

(c) A bacteria

(d) Special viruses (computer program) that spread using direct Internet connections

(x) Sniffers are software that illegally access data traversing across the network.

(a) True

(b) False

10.7 REFERENCES

1. http://eprints.qut.edu.au/13264/1/13264.pdf

2. http://www.delhicourts.nic.in/CYBER%20LAW.pdf

3. http://corporate.findlaw.com/business-operations/legal-issues-in-contracting-on-the-internet.html

4. http://www.nalsarpro.org/CL/Modules/Module%201/Chapter3.pdf

5.http://cis-india.org/internet-governance/blog/privacy/safeguards-forelectronic-privacy

6. http://cpe.ku.ac.th/~mcs/docs/E-Commerce_talk.pdf

7. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

8. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

10.8 SUGGESTED READINGS

1. Cyber and E-Commerce laws, P. M. Bakshi and R. K. Suri

2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

10.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Write an essay on the various issues involving in the cyber contract.

2. 'Security is a major issue in the cyber contract'. Comment.

3. Issues of privacy and security are discussed under the issue of technology in cyber contract. Explain.

4. What are the major security threats to the computer?

10.10 ANSWER SAQS

1. (i)(e); (ii)(f); (iii)(d); (iv) (a); (v)(a); (vi)(d); (vii)(a); (viii)(a); (ix) (d); (x) (a);