12

Cyber Laws

The fundamentals of e-commerce and finance rests mainly on the legality of e-contracts entered into between two or more parties. The rules and regulations are embodied in the Indian Contract Act, the Evidence Act, the Civil Procedure Code, the RBI Act 1934, the Bankers' Book of Evidence Act, and so on. However, all these embody rules regarding manual operations and paper-based documents.

Generally, commercial practice moves a few paces ahead of the statutes and it takes time for the laws to catch up. The same is true in a large measure about e-finance and e-commerce. The whole gamut of activities is yet to take deep root in the socio-commercial policy and with rapid technological advances being the order of the day; the lags are bound to be prevalent.

The earlier edition of this work concentrated more on legal provisions and the difficulties in bringing about parity between paper documents, manual procedures and their acceptability as evidence. During seminars and discussions, many participants wanted to know details regarding specific aspects like digital signatures, web penetrations, security lapses and enforcement of documents. Further, the changes introduced to Bankers' Book of Evidence Act, Contracts Act, and so on, were areas of concern rather than the broader aspects of the IT Act of 2000. Accordingly, this chapter has been tailored to suit these requirements and also to bring out the relevant features of the IT Act that are of great concern to the practicing financial services.

The incidence of cyber law pervades a number of areas, but we would concentrate on the following five aspects:

- The Contract aspect.
- The Intellectual Property aspect.
- The Security aspect.
- The Evidence aspect.
- The Criminal aspect.

In a sense 'cyber law' encompasses the whole gamut of legal statutory provisions that affect computers and computer networks. It concerns individuals, corporate bodies and institutions which

- are instrumental for entry into cyber space;
- provide access to cyber space;
- create the hardware and software which enable people to access cyber space and
- use their own computers to go online.

Potential litigants include telephone provider companies, regulatory agencies, personal computer companies, software companies, academic bodies and firms that have a presence on the internet.

Before proceeding further, it is necessary to mention that the technology scene is changing too rapidly for any legal provisions to keep pace with the changes. One hopes that the courts would give the legislation a much broader base than could be envisaged by the framers. We begin by looking at some of the future developments, which would have to be reckoned within the near future. The one thing that strikes even a casual observer is the new capabilities in processing speed, transport and storage. The constraining influence of bandwidth is beginning to diminish. Data can be moved far more efficiently than before. We may perhaps reach a stage where anything that can be digitized is delivered to any number of users and that too at negligible costs. The marginal cost of transport is zero.

Network technology is being used for an ever-growing number of tasks as we shift away from today's PC-based model. The desktop computer is becoming only one of the many platforms for accessing networks such as the internet. There would be small, lighter devices optimized for basic activities such as email, text communication, and so on. The 'language' used helps in turning these machines smarter. Computers and communication equipment communicate with each other and move in and out of the many networks of the infrastructure. Softwares can and do take over the tasks, which, normally, humans would have to perform. They connect to local networks, manage the flow of information and negotiate with other applications to achieve the tasks.

The impact of such changes on the economics of the internet has been considered in the chapter on internet economics. The following paragraphs would detail the specific aspects of law touched on earlier.

Questions of Jurisdiction

The first question that causes tremendous problems to the litigants is to have some understanding of a very perplexing issue of the scope of a court's power to hear particular disputes and to compel the parties involved to obey its commands.

It would be useful to mention that questions of jurisdiction are territorially based and they are difficult to translate to the internet. The word jurisdiction means many things and the broad umbrella of concepts that are covered can be summarized as follows:

- Power to legislate.
- Ability to serve the defendants a notice.
- Power to hear.
- Power to adjudicate.
- Subject matter of adjudication.
- Choice of law.
- Enforcement of judgments.

A brief discussion of Delhi High Court's judgement in the 'Banyan Tree' case is given below. The interested readers can find an exhaustive analysis of the case on the internet (spicyipindia.blogspot.com/2008/09/delhi-highcourt-considers-questions-of.html). Our purpose in citing the Indian case law is to demonstrate to the readers the complexity of issues, which otherwise appear to be simple. Further, it would be necessary to refer to case laws from countries like Canada, Australia, UK or the US. The issues are being examined from various angles and newer aspects are being considered. These cannot be ignored and would, over a period, fit some of our cases better than the body of decisions developed so far. All such matters have a vital bearing on the developments and students should pay attention to these aspects also.

Rather than going into a detailed review of case law it would suffice to mention some pertinent issues that have come up. Jurisdiction on the internet is an all-pervasive issue. Regardless of what substantive legal issue one is dealing with, whether it is intellectual property or privacy, jurisdiction issues would be key elements of that litigation. It would not be wrong to say that the internet is one big jurisdictional problem.

> Events on the Internet occur everywhere but nowhere in particular. Communications are engaged in by online personae who are human and real, but who are unreal in that they might not be traceable to any particular person. No physical jurisdiction has a more compelling claim than any other to subject these communications and events exclusively to these laws. (Post and Johnson 1996)

The Contract Aspect

The central point to remember is that the internet is a medium or a collection of media, which can be used for contracting. The law developed so far, does cover all the new elements it has been confronted with, but the law as it applies to the internet is far from settled yet.

Perhaps, the most suitable approach on the subject is Lord Denning's judgement in Entores Limited vs Miles Far East Corporation. The relevant portions of the judgment have been quoted for the readers to develop the right perspective.

> When a contract is made by post it is a clear law throughout the common law countries that the acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. There is no clear rule about contracts made by telephone or by telex. Communications made by these means are instantaneous and stand on a different footing …. The contract is complete only when there is acceptance of the offer. Any failure in hearing would result in the contract not being accepted. Same is the case when messages sent through teleprinters or telexes do not reach due to some failure of the system. The contract gets completed only when the messages are repeated and a proper acceptance received … In all the instances, the man who sends the acceptance knows that it has not been received or that he has reason to know it. But suppose he thinks that it has been received. —— The offerer in such cases is bound because he will be stopped from saying that he did not receive the message. (Lord Denning, Entores Limited vs. Miles Far East Corporation, 1955)

So far it has been assumed that the parties are present. The more likely events are that communication would be between the principals through the machines or through fax/email. However, it is possible that the senders and recipients may not be the principals, but servants with limited authority. The messages may have been sent out of office hours or there could be some default or defects at the recipient's end.

These difficulties can be constantly multiplied, but it has to be assumed that in the normal course of business, an acceptance sent by email/telex

should be treated as if it were an instantaneous communication between principals like a telephone conversation. Once the message has been received it is to be assumed that it has been delivered. The acceptor should take the required precautions to see that the acceptance is duly received. In conclusion, it could be said that: The 'offer' and 'acceptance of an offer' may be expressed by means of electronic records. As between the 'originator' and the 'addressee' of an electronic record, the expression/declaration of an intention 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. The concept of an 'Originator and Addressee', 'Acknowledgement of Receipt' and concepts of 'Time and Place of Despatch and Receipt' are dealt with in a genuinely different way and need to be highlighted.

1. Unless otherwise agreed to between the originator and the addresses the despatch of an electronic record occurs when it enters an information system outside the control of an originator.
2. Save or otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows:

If the addressee has designated a computer source for the purpose of receiving electronic records: *(a)* receipt occurs when the electronic record enters the designated computer resource and *(b)* if the 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.

The preceding section is not a complete reproduction of section 13 of the Information Technology Act. It has been included merely to stress the difficulties encountered in bringing about a functional equality.

The 'Functional Equivalent' Approach

The Model Law is based on a recognition that legal requirements prescribing the use of paper-based documentation constitute the main obstacle to the development of modern means of communication. The attempt was to overcome the impediments to electronic commerce by way of an extension of the scope of such notions as 'writing', 'signature' and 'original' with a view to encompassing computer-based techniques. Such an approach was used in a number of existing legal instruments, for example, in Article 7 of Model Law on Commercial Arbitration or in United Nations Commission

for Contracts for International Sale of Goods. It was also necessary to provide for developments in technology and communications applicable to trade laws without necessitating the wholesale removal of paper-based requirements or disturbing the underlying concepts.

The Model Law relies on an approach referred to as the 'functional equivalent' approach, which is based on an analysis of the purposes and functions of the traditional paper with a view to determining how these purposes or functions could be fulfilled through electronic techniques. Paper documents can be read, copied, preserved and would remain unaltered over time.

An electronic recorder can perform all these functions with a greater degree of reliability. The Model Law does not attempt to define a 'computer based' equivalent to a paper document. Instead, it singles out basic functions of paper-based form requirements with a view to providing criteria, which once met, enable the data-based messages to enjoy the same level of legal recognition as paper documents performing the same functions. The purpose in outlining the equivalence was to bring forth what the act was attempting, rather than be exhaustive.

The Information Technology Act 2000 is similar to the Model Law and the preamble acknowledges this fact.

> An act to provide legal recognition for transactions carried out by 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 Bankers' Book of Evidence Act 1891 and the RBI Act of 1934. (IT Act 2000)

The Act was passed to give effect to the resolutions of the United Nations General Assembly and to promote efficient delivery of government services by means of reliable electronic records.

We would now deal with one particular aspect viz. digital signatures and information security. The previous chapter dealt with security aspects at some length. This section will be restricted to problems of digital signature as a case of encrypted authentication. How a digital signature is created and how it achieves the same functionality as a hand written signature requires detailed explanation.

The Asian School of Cyber Laws defines digital signatures as 'an application of asymmetric cryptography'. Cryptography is the art of using codes and algorithms to scramble text so that it appears random to statistical

tests and can, therefore, be read by specified individuals only. It would be obvious that any communication in e-commerce transactions needs to confidential, must not be altered in transit and must have adequate authorization, Further, the contract agreement should necessarily have restricted access, certification about the genuineness of such a document and the time when it was sent. Also, any unauthorized entity viewing such a document should not become aware of the parties to these transactions. Apart from these there must be no repudiation of the document sent. Nor should it be possible to revoke it.

Any cryptographic method in transferring documents necessitates the use of keys to decode the message. Digital signatures rely on 'Asymmetric Cryptography'. The system involves use of a pair of keys: a public key which encrypts data and a corresponding private key for decryption.
The creation of digital signatures could be explained as a series of steps.

- A message is written.
- The message is encoded, the hash function takes a message of variable length and produces an output of a fixed length. If the information is changed even by one bit an entirely different value output is produced.
- The message is sent.
- The message is received and a key relating to the original algorithm is used to decode it.
- The message is then read.

Steps 2 and 4 are carried out with the help of a software sent by the sender.

On receipt of the message, the receiver computes the digest of the original message with the help of a hash function used by the sender. He then uses the sender's public key on the digital signature to compute another message digest. The receiver then compares the original with the message already obtained and only when it is identical is it proved that they are digitally signed by the sender and that the message is not altered. The need for all this arises because it is necessary to ensure that the message is not altered.

However, one has to be wary of what could be described as man-in-the-middle attack. You have to be sure that the public key is genuine and not a forgery. One way of solving the problem is to get a certificate which comes with a public key that helps one to verify that the key is genuine. Countries

like Germany and Sweden have elaborate procedures and precautionary requirements in place that are met by the certifying authorities. The legal issues, which would otherwise have complicated the whole question, have to some extent been resolved by the procedural guidelines.

Following are the detailed provisions regarding the status of certification under Indian law:

Certification authorities will be controlled by a controller who will be appointed by the central government. The duty of the controller would be to license, certify, monitor and oversee the activities of the certification authorities. Certificates issued by foreign authorities would be recognized in India if the laws of such a country have a level of reliability at least equivalent to that required in India.

It is likely that over a period of time, a number of vendors may come into the picture. Owing to the initial and on-going costs, it is unlikely that banks will opt to develop their own digital signatures and would have perforce to depend on outsourcing or purchasing this capability for their existing infrastructure.

A number of vendors are likely to emerge. Unfortunately, such vendors might market proprietary solutions that may not be compatible with the bank's other systems. Inter-operability now and in the future should be a primary consideration. Gartner Group estimates that 30–40 per cent of public key infrastructure deployments will fail within two years of launching because they fail to demonstrate value.

The trust placed in banks may lead to their setting up in the near future, a Certification Authority (CA) organization or could well find themselves using digital signatures that are unverifiable or information systems that have no technical support. Banks and financial institutions must perform a thorough check of the vendor who intends to provide a digital signature solution.

It needs to be emphasized that implementing the use of digital signatures requires adopting a new or augmented set of technologies, services and bank policies. Implementing digital signatures means implementing digital documents and associated requirements for document management, storage, access security, periodic hardware upgrades and disaster recovery facilities. Implementing digital signatures also leads to maintaining digital records and service digital documents.

Use of digital documents implies reasonable access being provided to the customers. Further, if remote access is to be provided, a secure information area will have to be provided.

A whole set of new issues come up when a bank decides to become a CA. The primary role of a CA is to issue and verify digital certificates.

There are some complex liability issues. Additionally hardware and software will become obsolete. The bank must upgrade and replace older equipment. The nature of 'second' documents would raise question about their admissibility. In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secured document is not altered since the specific point of time from which the record gained secure status.

The fact whether a secure procedure is commercially reasonable or not, shall be determined having regard to the procedure and the commercial circumstances at the time the procedure is used.

Evidence Aspect

This section will look into the question of acceptability in civil law cases. The detailed provisions have been deliberately quoted as bank and financial institution staff are very often required to present such documents in courts and it is necessary to have a proper understanding of the relevant provisions.

According to Articles 6, 7 and 8 of UNCITRAL Model Law, information shall not be denied legal effects, validity or enforceability solely on the grounds that it is in the form of a data message. Where the law requires information in writing, the requirement should be met by a data message if the information contained therein is accessible so as to be usable at a later date.

Article 9 of the Model Law provides the following regarding admissibility of evidence.

> In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic data message OR (b) if it is the best evidence that the person adducing it could be expected to obtain on the grounds that it is not in its original_form i.e., information in the form of a data message shall be given due evidential weight.

Of course, reliability of the manner in which the message was generated, stored or communicated, and the reliability of the manner in which its originator was identified, are the kind of factors that would be taken into account. The specific provisions contained in the IT Act 2000 relating to these aspects have been discussed in the following pages:

THE INDIAN IT ACT, 2000

Schedule II Information Technology Act, 2000—31*

Schedule II

(Section 91)

Amendments to the Indian Evidence Act, 1872

1. In Section 3,
   (a) in the definition of 'Evidence', for the words 'all documents produced for the inspection of the Court', the words 'all documents including electronic records produced for the inspection of the Court' shall be substituted;
   (b) after the definition of 'India', the following shall be inserted, namely, 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 1999'.
2. In Section 17, for the words 'oral or documentary', the words 'oral or documentary or contained in electronic form' shall be substituted.
3. After Section 22, the following section shall be inserted, namely:
   '**22A. When oral admission as to contents of electronic records are relevant.**
   Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.'
4. In Section 34, for the words 'entries in the books of account', the words 'Entries in the books of account, including those maintained in an electronic form' shall be substituted.
5. In Section 35, for the word 'record', in both the places where it occurs, the words 'record or an electronic record' shall be substituted.
6. For Section 39, the following section shall be substituted, namely:

* The amendments to IT Act 2008 could not be included in this book since the President's assent was not received when this book was sent for printing.

'**39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.**

When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters of papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.'

7. After Section 47, the following section shall be inserted, namely:

'**47A. Opinions as to digital signature when relevant**.

When the court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.'

8. In Section 59, for the words 'contents of documents' the words 'contents of documents or electronic records' shall be substituted.
9. After Section 65, the following sections shall be inserted, namely:

'**65A. Special provisions as to evidence relating to electronic record.**

The contents of electronic records may be proved in accordance with the provisions of Section 65B.'

65B. Admissibility of electronic records.

(l) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

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

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

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

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

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

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

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

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

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

(d) in any other manner involving the successive operation over that period, in whatsoever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

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

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

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

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,

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

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

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

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

10. After Section 67, the following section shall be inserted, namely:

'**67A. Proof as to digital signature**.

Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the

fact that such digital signature is the digital signature of the subscriber must be proved.'

11. After Section 73, the following section shall be inserted, namely:-

'**73A. Proof as to verification of digital signature.**

In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.'

Explanation: For the purposes of this section, 'Controller' means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 1999.

12. After section 81, the following section shall be inserted, namely:

'81A. Presumption as to Gazettes in electronic forms.

The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.'

13. After section 85, the following sections shall be inserted, namely:

'85A. Presumption as to electronic agreements.

The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

85B. Presumptions as to electronic records and digital signatures.

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(*a*) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(*b*) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85C. Presumption as to Digital Signature Certificates

The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.'

14. After section 88, the following section shall be inserted, namely:

88A. Presumption as to electronic messages

The Court may presumes that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.'

Explanation: For the purposes of this section, the expressions 'addressee' and 'originator' shall have the same meanings respectively assigned to them in clauses (b) and (z) of sub-section (1) of section 2 of the Information Technology Act, 1999.

15. After Section 90, the following section shall be inserted, namely:

'**90A. Presumption as to electronic records five years old**

Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This explanation applies also to section 81A.'

16. For section 131, the following section shall be substituted, namely:

'**131. Production of documents or electronic records which another person, having possession, could refuse to produce**

No one shall be compelled to produce documents in his possession or electronic records under this control, which any other person would be

entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.'

The next section analyses the provisions regarding the Bankers' book of evidence Act as modified by the IT Act 2000.

SCHEDULE III

(Section 92)

Amendments to Bankers' Book Evidence Act, 1891

1. In section 2—

(a) for clause (3), the following clause shall be substituted, namely:

'(3) "banker's books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in floppy, disc, tape or any other form of electro-magnetic storage device';

(b) for clause (8), the following clause shall be substituted, namely:

'**(8) "certified copy" means when the books of a bank—**

(a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title;

(*b*) consist of printouts of data stored in a floppy, disc tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'

2. After Section 2, the following section shall be inserted, namely:

'2A. Conditions in the printout

A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:-

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager;

(b) a certificate by a person incharge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorized change of date;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electromagnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person-in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, be relevant data.'

Intellectual Property Aspects

The Information Technology Act 2000, does not contain provisions relating to electronic copyrights or the protection of phonogram procedures against unauthorized duplication of their phonograms. Similarly, the

question of copyrights for software programmes have not been dealt with in the IT Act.

India is yet to legalize the functioning of online digital department stores, digital book stores and digital record and video shops. Once these are incorporated in the Indian IPR legislation, performers and makers of phonograms, software producers would have benefit of:

- legal remedy against misuse of copyright both direct and indirect in any manner or form;
- right of the owner of copyrights to make available to the public programmes/performance stored in electronic media, by interactive on-demand, online delivery methods;

Commerce on the internet involves the sale and licensing of intellectual property. To promote an effective environment, sellers must know that their intellectual property will not be pirated and buyers must know that they are buying authentic products and not pirated copies. The issues that are likely to come up would include the following:

- Liability of online service providers.
- Fair uses of copyright material.
- Effective patent systems.
- Standards for determining valid claims.
- Litigation due to trademarks.
- Similarity of internet domain names.

To conclude it can be said that in all these matters there is a need for detailed information about case law as is developing in various countries, particularly those where e-commerce has taken firm roots. Newer technology makes it imperative that those entrusted with the job of interpreting these laws, must be thoroughly familiar with the diverse aspects. We have drawn on two or three books dealing with cyber law and would like to acknowledge the great help received in writing this chapter. The books are:

- Yee Fen Lim, *Cyber Law: Commentaries and Materials*.
- Roodney D. Ryder, *Guide to Cyber Laws*.