Sarkar's
LAW OF
EVIDENCE

N.C. [illegible]
S.C. Sarkar
Prabhas C. Sarkar

Reprint [illegible]

Volume 1

SARKAR'S LAW OF EVIDENCE

Fifteenth Edition
Reprint 2004

(As Amended by Information Technology Act, 2000 and the Indian Evidence (Amendment) Act, 2002 (4 of 2003))

Volume 1

Sec. 1 To 100

Visit our website at:
www.wadhwain.com
E-mail : wadhwa@wadhwain.com

publishers

Wadhwa and Company Nagpur
Administrative Office
DD-13, Kalkaji Extn.,
Opp. Nehru Place,
NEW DELHI - 110 019 INDIA
Offices at :
NEW DELHI o NAGPUR o AGRA

authorised agents

Wadhwa Sales Corporation
Administrative Office
DD-13, Kalkaji Extn.,
Opp. Nehru Place,
NEW DELHI - 110 019 INDIA
Offices at :
NEW DELHI o NAGPUR

SARKAR'S LAW OF EVIDENCE

IN INDIA, PAKISTAN, BANGLADESH, BURMA & CEYLON

As amended by the Information Technology Act, 2000 and the Indian Evidence (Amendment) Act, 2002 (4 of 2003). Containing lucid, comprehensive, accurate and encyclopaedic information on Law of Evidence. This book solves all evidence quesitons quickly and saves valuable hours by enabling you to turn up any question instantly on account of its splendid arrangment.

by

M.C. Sarkar

and

S.C. Sarkar Judge, Calcutta Small Cause Court;
Author of Law of Civil Procedure, Law of Criminal Procedure & c.

and

Prabhas C. Sarkar Advocate, High Court, Calcutta;
Author of Law of Civil Procedure, Law of Criminal Procedure & c.

Fifteenth Edition* (Throughly Revised & Enlarged)

Reprint 2004 (As Amended by Information Technology Act, 2000 and the Indian Evidence (Amendment) Act, 2002 (4 of 2003), dt. 31-12-2002

by

Sudipto Sarkar, M.A., LL.M. (Cantab.) of Gray's Inn. Barrister, Senior Advocate, High Court, Calcutta

and

V.R. Manohar, B.Sc., LL.B., Former Advocate General of Maharashtra, Senior Advocate, Supreme Court of India, Chief Editor All India Reporter, Criminal Law Journal, Labour & Industrial Cases, Taxation Law Reports, AIR Manual, Ex Dean Faculty of Law, Nagpur University, Ex Chairman Bar Council of Maharashtra.

Volume 1

THE INDIAN EVIDENCE ACT, 1872

Sec. 1 To 100

* Fifteenth Edition 1999.

First Edition	1913
By M.C. Sarkar S.C. Sarkar	
Second Edition	1924
By S.C. Sarkar	
Third Edition	1925
By S.C. Sarkar	
Fourth Edition	1929
By S.C. Sarkar	
Fifth Edition	1932
By S.C. Sarkar	
Sixth Edition	1939
By S.C. Sarkar	
Seventh Edition	1946
By S.C. Sarkar	
Eighth Edition	1949
By S.C. Sarkar	
Ninth Edition	1953
By S.C. Sarkar	
Tenth Edition	1959
By S.C. Sarkar	
Eleventh Edition	1965
By S.C. Sarkar	
Twelfth Edition	1971
By Prabhas Sarkar Sudipto Sarkar	
Reprint	1977
Thirteenth Edition	1980
By Prabhas Sarkar Sudipto Sarkar	
Reprint	1990
Fourteenth Edition	1993
By Sudipto Sarkar V.R. Manohar	
Reprint	1994
Fifteenth Edition	1999
By Sudipto Sarkar V.R. Manohar	
Revised Reprint	**2000**
Reprint	2002
Reprint	**2003**
Reprint	**2004**

Printed Pages
—Volume 1—1670 (approx.)
—Volume 2—1312 (approx.)
Price in India
—Volume 1 Rs. 1195.00
—Volume 2 Rs. 1195.00
Price abroad £ 200 $ 300 (US)
(For the set of 2 Volumes)

Publishers : Wadhwa and Company,
Law Publishers,
Agra/Nagpur/New Delhi

Paper-Export Stuff

Printed at
WIN Offset Printers
B-193, Okhla Industrial Area, Phase I
New Delhi 110 020

Printed and bound in India.
15141312110987654321

preface to the fifteenth edition

The present edition comes after a gap of nearly five years. Though it is a shorter period as compared to the gap between the earlier editions, this period of five years has been of greater value to the developments in the law of evidence. During this period the subject has grown not only quantity-wise by accumulating a large number of cases and statutory changes, but also quality-wise in the sense that the modern scientific techniques of investigation and the advancement in information technology have brought about sea changes in this field resulting in re-examination and revision of a number of fundamental doctrines. Some of the fundamental doctrines were the best evidence rule; the necessity of direct evidence; prohibition of hearsay personal appearance of witnesses; precedence of documentary evidence; the concept of a document and privileged communications beyond disclosure. These doctrines are no longer fundamental to the subject, but are considered to be only of functional nature. The law of evidence governs the modes and methods for provision of facts and information to enable a judicial conclusion. It is a technique for transmission of information. The subject remained interwoven with information technology. Therefore, it has always remained responsive to the improvements in information technology. The more stupendous such changes, the more rapid the changes in the law of evidence.

As this edition progressed in its search for the recent judicial output on the subject, it was found that electronic and video links have changed the requirement of personal appearance of witnesses, that the traditional concept of a document has been transformed by computer records and tapes which can be retrieved on the screen or paper, that the rigid rule of hearsay has had to make concessions in favour of technological evidence, and that the probative value of the information is a more important consideration than the earlier rigid doctrines. In this search for latest developments for the enrichment of this edition, cases and materials from many other countries and judicial systems have been traced in addition to those of India. Such countries include Australia, New Zealand, Malaysia, Singapore, Hongkong, England, European countries, Canada, Nigeria and South Africa.

Apart from the new additions, the existing text has been subjected to a thorough reading and revision. A lot more headings and sub-headings have been added with a view to help the readers to locate the topic of their need more conveniently and quickly.

The contribution of the Indian judiciary in this field has been collected from all sources comprising All India Reporter and also Regional Journals. An exhaustive view of each and every worthwhile case has been presented.

(Contd.)

preface to the fifteenth edition (contd.)

Materials have also been taken from leading articles on the subject appearing in the standard legal journals. Topics like circumstantial evidence, value of dying declaration and expert opinion, standards of proof, estopped competence of witnesses and protection of witnesses from aggressive cross-examination particularly when the victim of rape is being cross-examined, have attracted a good number of decisions creating some new trends.

We are thankful to the publishers for the excellent production and maintenance of laudable marketing record which enables us to present revised editions at shorter intervals. In addition to this, the research and development division of the publishers was instrumental in conducting the praiseworthy search for cases for which we remain immensely grateful.

22nd November, 1998

Sudipto Sarkar
V.R. Manohar

preface to the thirteenth edition

Since the last edition nothing has happened in this country with regard to the amendment of Indian Evidence Act, 1872 apart from the introduction of a bill, the Indian Evidence Amendment Bill, 1979 which is not yet of statutory force. The bill proposes certain amendments to Chapter II of the Act.

A statutory amendment has taken place in England by the Civil Evidence Act, 1972 relating to the admissibility of expert and opinion evidence.

Some major changes have been made in England by case-law and some changes have also taken place here.

Perhaps the decision with the most far reaching effect here is the one delivered by the Supreme Court in *Dastane v. Dastane*, AIR 1975 SC 1534 which appears to decide that standard or proof in matrimonial matters is the preponderence of probability as in civil cases. The scope of the decision is far from clear in view of various other judgments to the contrary including some earlier Supreme Court judgments.

As in the earlier editions many English decisions have been incorporated wherever thought applicable and useful.

We are very happy to say that the 12th edition, the first since the death of the author was so well received that it became out of print within a short time and we had to bring out a reprint edition in the year 1977 which also became out of print in 1978. We hope that readers and users of the book would continue to maintain their confidence in the book as they have done in the past.

Addenda 1 and 2 contain cases that came out while the book was passing through the press. Decisions up to July, 1981 have been incorporated in this edition.

We shall be grateful if readers coming across any error or omission bring it to our notice.

Calcutta
15th Sept. 1981

PRABHAS C. SARKAR
SUDIPTO SARKAR

preface to the eleventh edition

In the present edition the book has been very carefully revised throughout and some of the principal topics have been more fully treated. Not only have case-laws been brought down to date of publication but the statements of law under each section have been scrutinised with care with a view to ensure accuracy. Necessary suggestions have been made on obscure points or points not covered by precedents and comments have been offered on a few unsatisfactory decisions of the higher courts.

In the preface to the eighth edition of the work published in January, 1949, I pleaded strongly for a thorough reform and rethinking on the law of Evidence and the appointment of a Law Commission for the purpose. The latter has since been established but no revision of the Indian Evidence Act has been undertaken by that body and that Act has practically remained unamended since it was passed 93 years ago.

Upon reading my preface to the 8th edition, Mr. P.V. Rajamannar, the then Chief Justice of the Madras High Court, wrote me in the course of a letter dated the 25th April, 1949 :

> "The preface to the present edition (8th) contains a plea for the reform of law of Evidence which is thought provoking and deserves attention. I entirely agree with the learned author that there is much scope for legal reform, particularly, in the law of Evidence and I had occasion to emphasise the need for setting up an independent expert body to study and ascertain the modifications which are necessary having regard to the altered conditions of life at the present time. As the learned author says 'laws cannot remain in a static condition if it is to keep pace with the march of society and the progress of knowledge and civilization'. Mr. Sarkar has indicated some instances in which the law of Evidence needs reconsideration and reform, the most important of which is the recognition of the competence of an accused to testify on his own behalf."

As to the competency of an accused to testify for the defence, it was at long last recognised by the legislature by a slovenly addition of section 342A to the Criminal Procedure Code, 1898 (by Act 26 of 1955) which leaves unsolved many important problems like the answering of any criminating question by the accused in his cross-examination, or any question tending to show that the accused has committed or been convicted of or been charged with any offence other than that wherewith he is then charged, or is a bad character &c. &c. These and many other questions would naturally crop up when an accused comes to offer himself as a witness for the defence. These and other intricate questions have been dealt with in the English Criminal Evidence Act, 1898 (61 & 62 Vic. c. 36) section 1(e), (f), (g) &c. of that Act. Section 342 of the Burma Criminal Procedure Code as amended by Burma Act, 13 of 1945, which proceeds on the lines of the English Criminal Evidence Act, 1898, is a better piece of legislation.

There has been no worthwhile amendments to the Indian Evidence Act since 1872, while during this long interval legislation introducing reforms in the law of Evidence has gone far ahead on many occasions in England and several instances may be cited. The presumption relating to ancient documents has been reduced to 20 years by s. 4

(contd.)

of the Documentary Evidence Act, 1938 (1 & 2 Geo. 6. c. 28). This Act has effected many reforms by modifying the common law and is applicable to civil proceedings. It has modified the rule excluding hearsay in documents. In *Bhogilal v. State*, A 1959 SC 356 the Supreme Court had occasion to notice one of its provisions. It was observed by that court that a change was, however, introduced in the English law by the Evidence Act, 1938, which provides than in any civil proceeding where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact, shall on production of the original document, be admissible as evidence of that fact, if the maker of the statement has personal knowledge of the matter dealt with by the statement and if he is called as a witness in the proceedings. Provided that the last condition may be dispensed with if the person cannot for any reason be called as a witness. In cases of undue delay or expense, the court has been further empowered to admit such a statement in evidence notwithstanding that the maker is available as a witness and that the original is not produced, if there is produced a certified copy of the original if prescribed conditions are satisfied [s. 1(2)(*b*) of the Act]. The conditions as to the death of the person or the statement being against the interest of the maker or made in the course of business (as in s. 32 of the Evidence Act) has also been dispensed with.

The overstrict law as to the proof of an attested documen. in s. 68 of the Evidence Act has been considerably altered in England by the Evidence Act, 1938 (1 & 2 Geo. 6. c 28). Under s. 3 proviso of this Act except wills and other testamentary documents, instruments which are required by law to be attested, instead, of being proved by an attesting witness, may be proved as if no attesting witness were alive; that is by proof of an attestor's handwriting. The introduction of such law in India is long overdue and the continuation of the former English law promotes needless perjury in many cases which is avoidable.

The object of the English Act, 1938, is to lighten the burden of proof in various cases and to save time and expense by dispensing with the formality of strict compliance with the rules regarding the proof of certain documents.

In a despatch by Reuter dated the 24th September, 1964, the following news was announced (as reported in the Statesman of 25/26 September) :

> "England's Law of Evidence covered by Acts of Parliament which mostly dates back to the 19th century is to be reviewed.
>
> The Law of Evidence regulates such matters as what is admissible for the purpose of establishing facts in legal proceedings; the manner in which the facts may be proved; and the weight to be attached to particular kinds of Evidence.
>
> It is one of the complex branches of the English Law.
>
> In deciding on the review, Britain's Home Secretary, Mr. Henry Brooke and the Lord High Chancellor, Dilhorne believe special scrutiny is needed on the rules restricting the admission of hearsay evidence; on the need for proof in criminal

(contd.)

proceedings of facts admitted by the defence; on rules governing the admissibility in criminal proceedings of questions tending to show that the accused has committed other offences or is of bad character; and on the extent to which documentary evidence may be admitted.

The review will be conducted by the Law Reforms Committee and the Criminal Law Revision Committee."

The above extract shows how deeply concerned the Government of Britain is to review and effect reform in the law of Evidence periodically and systematically. But conditions in this country are otherwise and legislative wheels move here at a painfully slow pace.

It is more than high time that a thorough review of the Indian law of Evidence were taken up as speedily as possible. This task should be undertaken not by the Law Commission alone, but also by an independent body of experts, who have made a special study of this branch of law, should be co-opted and associated with it. These experts and the Law Commission should deliberate what changes and modifications are needed in the law of Evidence at the present time. There is abundant scope for reviewing and reshaping the law of Evidence in the light of enlightened legislation elsewhere and particularly in the Britain as the Indian Evidence Act is entirely based on the English law of Evidence which was in vogue in the seventies.

It is unquestionably the duty of the Indian Legislature to take up the work of an extensive reform and reconsideration of the law of Evidence, but it is apprehended that it will again be a lone voice in the wilderness as has happened during the past sixteen years.

Addenda 1 and 2 contain cases that came out while the book was passing through the press. Case-laws have been brought down to January, 1965.

Mr. P.C. Sarkar, Advocate, High Court, has rendered valuable assistance in the reading of proofs and has also helped me in numerous other ways.

I shall be grateful if any reader coming across any typographical or other error or omission in the book, brings it to my notice (care of the Publishers).

March, 1965,
Calcutta

S.C. SARKAR

To the Second Edition, by Mr. Justice C. WALSH, M.A., K.C., High Court, Allahabad, Author of "The Advocate", "Revision & Extraordinary Jurisdiction", &c.

It is not easy to say anything which is either new or valuable about the Indian Evidence Act. Nor to a lawyer, whose experience has been gained chiefly in the English courts, it is easy to work by a Code of the Law of Evidence. The English practitioner who has read "Taylor on Evidence" from cover to cover, or who has attempted anything like complete study of the rules of Evidence, must be scarce. Once he has mastered the fundamental truths that the English law requires the best evidence, and does not permit hearsay, the problems which present themselves for solution in the course of daily practice require little more than the application of logic and common sense.

The thoroughness with which cases in England are prepared before they come into court, and the preliminary skirmishes which take place in Chambers over interlocutory applications in most cases of any importance, result in the settlement of many of those subsidiary points which arise in the majority of cases, before the trial begins. It has been truly said that cases are often won or lost in Chambers. The machinery of "Discovery," if rightly understood and utilised, extracts from either side all the material documents in its possession, and with the aid of inspection and the supply of copies, enables both sides to go to trial fully equipped with all the relevant documents relied upon by either party. Nearly all questions relating to the relevance of the documents have already been determined in Chambers before the trial begins. Facts within the knowledge of one party, but unknown to the other have been disclosed, and elucidated, by admissions and interrogatories. Thus nearly all the cards are on the table, and the risk of "surprise" is reduced to a minimum. To pursue the analogy of the card-table, most suits are fought out, as it were, in a game of "double-dummy". Each party is fully aware of the strong features and the weak spots in both its own and its opponent's armoury respectively, and it rarely happens that any question as to the admissibility of a document, or the relevance of a fact, is still outstanding when the hearing begins. Counsel on either side, responsible for the preparation, and also, when no leader is employed, for the conduct of the case in court, have advised on evidence, and have mapped out for the guidance of the solicitor, who is putting the final touches to the preparation of the case, a ground plan of what is required to establish the issues essential to success.

The value of perfecting your tackle in this way before the real struggle begins cannot be over-estimated. Not only is each side fully armed at all points which foresight, judgment and experience can suggest, but the hearing is concentrated on the main issue, or pivot of the dispute, and is confined within limits which eventuate in a saving to the parties of time and money — the one essential in all litigation if the administration of the law is to merit and maintain the confidence of the commercial public. Moreover, the exhausting and embarrassing struggles over side-issues and technical objections are almost wholly eliminated. It is recognised by every practitioner as a matter of first importance that a defeat at the trial upon a subsidiary point is injurious to the chance of success upon the main issue. To tender evidence which is ultimately rejected, and to struggle successfully for its admission, necessarily create in the mind of the tribunal an impression of distrust as to the merits of the residue of your case.

(contd.)

If your other evidence is adequate, it is superfluous to offer supplementary proofs which are open to serious objection. Again, to object unsuccessfully to evidence tendered by the other side is liable to produce a similar impression. You seem to be anxious to exclude something which you have reason to fear. The consequence is that the best practitioners avoid raising objections unless they are confident of success, and do not risk a decision against them excluding evidence which is not essential. It may therefore be said that the combined effect of the mutual tact and reasonableness of the opposing forces is, in almost all cases which are skilfully conducted, to eliminate subordinate controversies upon points of evidence. It becomes in effect a question of practice and procedure rather than one of substantive law.

It is, therefore, to points of practice rather than to principles underlying the Law of Evidence that I can most usefully address myself. The student of law will find in the pages of this exhaustive work all that he needs to know. The practitioner should know the Evidence Act by heart, so that he is never at a loss, when called upon in court, to give chapter and verse for what he is doing. He should take the actual sections as his sole guide, and leave case-law as far as possible, alone. The conduct of the trial is the translation into action of his client's paper-case, and he should use the Evidence Act as the translator uses his dictionary. Like the careful mariner, he should lay out his course and clearest passage which he can see to lead him to his goal; and he should steer his way along this course, checking his progress and verifying his results as he moves from stage to stage of his journey, until he reaches the accomplishment of his task, without deviating from his plan, jettisoning his cargo.

For this purpose, he must realize from the first, and never forget it that it is the documentary evidence which constitutes the strength of most cases. He must start by asking himself what documents are necessary to establish his client's case; where they are ; how they are to be obtained; and what is the mode of proof required by law to establish each one of them. Next, he must ascertain, by the valuable machinery, provided in the Civil Procedure Code, known as "Discovery", whether any other documents exist in the possession of his opponent, of which he has no knowledge, and which may assist, or injure his client's case. I have always said that any practitioner who went into Court without having first raked his opponent fore-and-aft to ascertain what relevant documents were in his possession, ran a grave risk, and if misfortune resulted in consequence of the omission, was guilty of a high degree of negligence. No practitioner knows how far his client may have forgotten, or deliberately ignored, the existence of some embarrassing document with which the other party is armed and which may at some later stage be sprung upon him by surprise, and the knowledge of which in the early stages of preparation would have enabled him to frame his case on the right lines. The obligation laid upon each party by the Civil Procedure Code to file in Court all documents on which he relies is not, in itself, a sufficient guarantee against the possibility of a miscarriage. On the other hand, it is not always necessary to disclose to your opponent, before the day for filing arrives the existence of material documents adverse to his case. And it is often undesirable to do so unless he, in his turn, presses for an affidavit of documents. Even if he does so, there is no obligation upon a party to file or disclose documents which are in the sole possession of a mere witness, who is to be called to produce them, and it would be quixotic to do so if a material advantage were to be gained by keeping them secret.

(contd.)

The next important step is to decide what witnesses are necessary to prove, support, or elucidate the documents which are essential to success. For this purpose, it is well to submit all such necessary witnesses to a preliminary examination, so as to refresh their memories, or to test their evidence in the presence of the document itself, or a copy thereof. A witness called in relation to a document should never be exposed to the risk of "surprise". This process may be called "dove-tailing" the oral evidence into the documentary. As often as not, it turns out to be superfluous. But this is no excuse for omitting the step. One never knows. There may be some peculiarity about the document itself, or about its execution, which cursory examination of it has not discovered, or which only the renewal of his acquaintance with it by witness may disclose. The discovery may occur from some chance remark. It may necessitate the summoning of some additional witness by way of corroboration, or the preparation, by way of anticipating the attack which is certain to come, of a true but involved explanation. Such preparation should precede the trial. It may afterwards be unavailable, or unconvincing when hastily attempted in the surprise and confusion of a first discovery made in the course of the trial. For the same reason, it is essential when examining a witness in relation to a document to which he was a party, or which he is called to support or explain, to put it into his hand, and to take him through it while he is in the box, so that he is able to give clear and intelligible answers. No witness should ever be asked a question relating to a document which is in court, without having it in his hand, to refer to. I have seen cases last, or seriously hampered in the Appellate Court, by the neglect of this obvious precaution. When the trial judge comes to write his judgment, or the Appellate Court comes to review the whole evidence, a serious *lacuna* is discovered which there is nothing to fill.

In this connection there is one slovenly practice of which I have known some Subordinate Judges of my Province to be guilty, and which seems to me of sufficient importance to deserve a word or two of comment. I do not suggest that it is general throughout India, but it does happen, and it is valuable as an illustration of how *not* to do it. The filing of the documents, and the arguments relating to their admission of relevance, sometimes take place on what is called the first day of hearing, when the issues are settled. It takes place as an independent ceremony detached from the remainder of the hearing. Sometimes elaborate arguments are allowed. This is wrong. The process should be speedy and superficial. Any difficult question of admissibility should be dealt with by allowing the document to be filled *de bene esse*, subject to any formal objection at the trial, when after argument the judge should give his final ruling, and state his reasons for admission or rejection in his judgment. Some sort of desultory weeding takes place, but it is not followed upon by a ruling at the trial. The resulting balance is treated as the documentary evidence in the case, and dates are fixed for the summoning of witnesses. When these gentlemen arrive, they proceed to transact their business—one might almost say, to perform their drill—without reference to the documents which have now been put temporarily on the shelf. One might just as well send infantry into battle without artillery. It is as though a General commenced operations without a preliminary bombardment a week before the battle, and then packing away his guns proceeded to employ his infantry at his leisure, after a decent interval for reflection. What is the result? Documents are not tendered in evidence. They are "on the record". The practice of "putting them in," of discussing them, and of trying to understanding them in the presence of the witnesses who can explain

(contd.)

them and of dove-tailing them into the story is neglected. They make their re-appearance in a kind of "salvo," or valedictory bombardment, during the final arguments which precede the judgment.

At this later stage, the judge wakes up to the fact that the law requires him to endorse on each document the decision at which he has arrived upon its admissibility. He hastily runs through the task, endorsing as a rule merely the name of the party—plaintiff or defendant—who produced it, and a date. I frequently found the date to be the same date as the judgment, and the same date for all documents. Whatever may be the right way of dealing with documents at the trial it is certainly not this. In the few original trials which I have heard in India, my practice has always been to insist upon the officer of the court keeping two files; one "omnibus" file, for all documents filed by the parties in compliance with the Civil Procedure Code before the hearing, and the other to which each document is transferred *seriatim* as it is put in during the evidence. On each of these I endorse an exhibit number, with the name of the witness in the course of whose evidence it was "put in," or proved; any admission by the opposite party, or ruling by myself as to its admissibility; and the date. This plan, to say the least of it, affords the Appellate Court a clear "bird's-eye-view" of how the documentary evidence was dealt with at the trial. People too often forget that the object of litigation is to elucidate and not to obscure.

For one who has rarely in the course of his professional career consulted any authority upon a question of evidence, and, content with the provisions of the Act, has never been driven to do so in the course of his judicial experience in India. I marvel at the wealth of reported cases which have grown up round this Act. Several pages of this work are devoted to the simple proposition that an Act must be "construed strictly". I do not know even what this means. Everything ought to be done strictly, particularly in the law. The judicial task is complete when the Judge, or Bench, has applied to the language of a section, the natural meaning of the words. It is astonishing that it should be thought necessary to deliver a thoughtful judgment, and even to cite authorities, explaining that section means what it says. It is more surprising that any one should think it worthwhile to report the case. I fear the responsibility rests rather with the reports and with editors of reports, particularly unofficial reports. I have been amused at times to renew acquaintance with my own platitudes, solemnly recorded with all the majesty and importance of "an authority," after I supposed that I had said farewell to them for ever in the necessary but obvious reasons for a decision.

The text-writer has no option but to produce and arrange his wealth of learning, and the student will benefit by a perusal of the vast range of subjects covered by the author of this work. A book so well known as to have reached a second edition requires little more to recommend it. I only hope that its many readers will, bestow upon its study one tithe of the industry and zeal which has been lavished upon its compilation.

ALLAHABAD,
January, 1924

CECIL WALSH

prefatory note to the second edition

Though a new edition, this is in some respects a new book. The first edition was published in 1913 and the reception accorded to it far exceeded the author's highest anticipations, with the result that an edition of several thousands was exhausted within the space of two years. Numerous were the enquiries received in the interim from far and near, regarding the publication of the new edition. The present edition, and in fact several editions, should have been published long long ago and I owe an explanation for my inability to take up the work earlier. Many things stood in the way, but I would give two principal reasons. A judicial officer holding my office has a very hard lot to bear. The manifold duties of a judge absorb most of my time and even encroach upon my leisure hours at home. Secondly, I was not prepared to send out the book by merely adding new cases. That would have been a comparatively easy affair. I wanted to revise and arrange the whole book and re-write portions of it, which meant considerable time. This has now been done. The amount of labour involved will appear from the fact that I had to work incessantly for more than two years.

The commentary portion has been throughout re-written. As was observed in the preface to the first edition, the Indian Evidence Act contains certain abstract rules taken mostly from the English Law, arranged in the form of express propositions. The meaning of the rules, their object, the reasons on which they are founded, their gradual development and their proper application cannot be fully comprehended without a previous acquaintance with the law from which they are chiefly drawn. I have therefore referred copiously to English and foreign cases in order to explain the meaning and scope of the sections.

The bulk of the book has been increased by almost double the number of pages in the first edition.

* * * * *

The utility of the book has been considerably enhanced by the pages containing a discourse on the practical application of the rules of evidence, contributed by the Hon'ble Mr. Justice C. Walsh, M.A., K.C., of the Allahabad High Court, His "FOREWORD" contains hints on points of practice and procedure picked from his long experience at the Bar and Bench, which judges and practitioners will find of inestimable value. His racy style makes his writing pleasant reading and is peculiarly well suited to bring home the lessons he wants to impress. I take this opportunity of giving public expression to my deep debt of gratitude for the interest he has taken in the book by kindly making time to write the pages in the midst of various preoccupations and for other acts of kindness.

* * * * *

Calcutta,
January, 1924

S.C. SARKAR

preface to the first edition

The Indian Evidence Act is unquestionably the most important enactment of all the codified laws of the land. The one thing on which the decision of every case, civil or criminal, depends, is evidence and a thorough understanding of the principles of the law of Evidence, is an accomplishment that every lawyer or judge must possess. It has to be applied in almost every matter that comes before the judge, and its usefulness in civil and criminal cases is the same. A mastery, therefore, of the principles and rules of the law of Evidence, is indispensable to all grades of judges, magistrates, counsel, etc. Even police and other ministerial officers are required to make themselves acquainted with some of its rules.

The codified law of Evidence in British India contains certain abstract rules arranged in the form of express propositions mostly taken from the English law of Evidence. But as all that is contained in the voluminous text-books on English law has been squeezed into the four corners of the Act comprising 167 sections only, it is no wonder that the sections have become extremely condensed and abstruse. A knowledge of the principles and reasons on which they are founded, is therefore essential, before one can expect to understand them fully. As the Act is drawn chiefly from the English law, a previous acquaintance with that law affords much help in grasping the abstract rules of the Evidence Act; in fact, a reference to that law is essential for a thorough comprehension of the origin, the history, the gradual development, and the reasons of those rules which form the basis, of the law of Evidence and which, as Lord Erskine said are founded "in the charities of religion, in the philosophy of human nature, in the truths of history, and in the experiences of common life".

I have therefore striven to explain the sections as clearly as possibly by numerous apt and long abstracts from many standard works

* * * * *

Now a word as to the genesis of the work. It need hardly be said that I have not the remotest intention to place it in competition with the well-known existing editions. While I was a judge, it was represented to me by the lawyers of many places that the want of a moderate-sized book on Evidence dealing exhaustively with the subject and affording practical help to the understanding and application of this difficult branch of legal study, at a cheap cost, was keenly felt. I took up the idea, but found no possible means of taking up the work in hand, as the enormous duties of a judicial officer took up the whole of my time. At the same time, I began to make the necessary studies and to collect materials, in the hope that it might be possible to produce the work at some future period. After I retired from the service, my son Subodh Chandra Sarkar, B.L., persuaded me to take up the work, promising his help and co-operation. I received assistance from him in all stages of the work, and had it not been for his labours it would have been scarcely possible for me to accomplish the task at this period of my life.

* * * * *

Calcutta,
August, 1912

M.C. SARKAR

SARKAR'S
LAW OF EVIDENCE

Fifteenth Edition 1999
Volume 1
Sec. 1 To 100

SARKAR'S

LAW OF EVIDENCE

FIFTEENTH EDITION (REVISED REPRINT 2000)

General Contents of Volume 1

The Indian Evidence Act, 1872

PART I

RELEVANCY OF FACTS

NOTE : PART III— **PRODUCTION AND EFFECT ON EVIDENCE,** Section 101, onwards continued in Volume 2.

STOP PRESS-2000

APPENDIX E

INFORMATION TECHNOLOGY ACT, 2000

(Received the Assent of the President on 9th June, 2000)

ACT NO. 21 OF 2000

ARRANGEMENT OF SECTIONS

CHAPTER I

PRELIMINARY

CHAPTER II

DIGITAL SIGNATURE

CHAPTER III

ELECTRONIC GOVERNANCE

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS

Section Page

Section Page

Section

INFORMATION TECHNOLOGY ACT, 2000

(Received the assent of the President on 9th June, 2000)

ACT NO. 21 OF 2000

An [9th June, 2000]

ACT

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, the Indian Evidence Act, 1872, *the Banker's Books Evidence Act,* 1891 *and the Reserve Bank of India Act,* 1934 *and for matters connected 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 favourable 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 give 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 Fifty-first Year of the Republic of India as follows.

CHAPTER I

PRELIMINARY

S. 1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) 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.

(4) Nothing in this Act shall apply to,—

(*a*) a *"negotiable instrument"* as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881);

(*b*) a *"power-of-attorney"* as defined in section 1A of the Powers-of-Attorney Act,1882 (7 of 1982);

(*c*) a *"trust"* as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1982);

(*d*) a *"will"* as defined in clause (*h*) *of* section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called;

(*e*) any contract for the sale or conveyance of *"immovable property"* or any interest in such property;

(*f*) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

NOTES

This clause provides for the documents, records or information which has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form. (*Clause 1* of the Information Technology Bill, 1999)

Clause 1(*4*)(*f*) of the Bill empowers the Central Government to notify any class of documents or transactions in the Official Gazette to which the provisions of this Act will not apply. (*Memorandum Regarding Delegated Legislation* of the Information Technology Bill, 1999).

STATEMENT OF OBJECTS AND REASONS

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. Businesses 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 conduct 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 legal 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.

2. The United Nations Commission on International Trade Law (UNCJTRAL) adopted the Model Law on Electronic Commerce in 1996. The General Assembly of United Nations by its Resolution No. 51/162 dated 30th January, 1997 recommended that all States should give favorable considerations to the said Model Law when they enact or revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Pursuant to a recent declaration by member countries, the World Trade Organisation is likely to form a work programme to handle its work in this area including the possible creation of multilateral trade deals through the medium of electronic commerce.

3. There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures. This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. It is also proposed to provide for a regulatory regime to supervise the Certifying Authorities issuing Digital Signature Certificates. To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislation.

4. With a view to facilitate Electronic Governance, it is proposed to provide for the use and acceptance of electronic records and digital signatures in the Government offices and its agencies. This will make the citizens interaction with the Governmental offices hassle free.

5. It is also proposed to make consequential amendments in the Indian Penal Code and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions. It is also proposed to amend the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks and the Bankers' Books Evidence Act, 1891 to give legal sanctity for books of account maintained in the electronic form by the banks.

6. The proposal was also circulated to the State Governments. They have supported the proposed legislation and have also expressed urgency for such legislation.

7. The Bill seeks to achieve the above objectives.

S. 2. Definitions.

(1) In this Act, unless the context otherwise requires,—

(*a*) *"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;

(*b*) *"addressee"* means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(*c*) *"adjudicating officer"* means an adjudicating officer appointed under sub-section (*1*) of section 46;

(*d*) *"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;

(*e*) *"appropriate Government"* means as respects any matter,—

(*i*) enumerated in List II of the Seventh Schedule to the Constitution;

(*ii*) 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;

(*f*) *"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;

(*g*) *"Certifying Authority"* means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(*h*) *"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;

(*i*) *"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;

(*j*) *"computer network"* means the interconnection of one or more computers through—

(*i*) the use of satellite, microwave, terrestrial line or other communication media; and

(*ii*) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(*k*) *"computer resource"* means computer, computer system, computer network, data, computer data-base or software;

(*l*) *"computer system"* means a device or collection of devices, including input 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;

(*m*) *"Controller"* means the Controller of Certifying Authorities appointed under sub-section (*7*) of section 17;

(*n*) *"Cyber Appellate Tribunal"* means the Cyber Regulations Appellate Tribunal established under sub-section (*1*) of section 48;

(*o*) *"data"* means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised 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;

(*p*) *"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;

(*q*) *"Digital Signature Certificate"* means a Digital Signature Certificate issued under sub-section (*4*) of section 35;

(*r*) *"electronic form"* with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, Computer Generated micro fiche or similar device;

(*ra*) *"Electronic Gazette"* means the official gazette published in the electronic form;

(*s*) *"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;

(*t*) *"function"*, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(*u*) *"information"* includes data, text, images, sound, voice, codes, computer programmes, software and data-bases or micro film or computer generated micro fiche;

(*v*) *"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;

(*w*) *"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;

(*x*) *"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 (*1*) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(*y*) *"licence"* means a licence granted to a Certifying Authority under section 24;

(*z*) *"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;

(*za*) *"prescribed"* means prescribed by rules made under this Act;

(*zb*) *"private key"* means the key of a key pair used to create a digital signature;

(*zc*) *"public key"* means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(*zd*) *"secure system"* means computer hardware, software, and procedure that—

(*a*) are reasonably secure from unauthorised access and misuse;

(*b*) provide a reasonable level of reliability and correct operation;

(*c*) are reasonably suited to performing the intended functions; and

(*d*) adhere to generally accepted security procedures;

(*ze*) *"security procedure"* means the security procedure prescribed under section 16 by the Central Government;

(*zf*) *"subscriber"* means a person in whose name the Digital Signature Certificate is issued;

(*zg*) *"verify"* in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(*a*) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(*b*) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) 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.

NOTES

This clause defines the various expressions occuring in the Bill. (*Clause 2* of the Information Technology Bill, 1999)

CHAPTER II

DIGITAL SIGNATURE

S. 3. Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) 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 every time the algorithm is executed with the same electronic record as its input making it computationally infeasible —

(*a*) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(*b*) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

NOTES

This clause provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message. (*Clause 3* of the Information Technology Bill, 1999)

CHAPTER III

ELECTRONIC GOVERNANCE

S. 4. 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—

(*a*) rendered or made available in an electronic form; and

(*b*) accessible so as to be usable for a subsequent reference.

NOTES

This clause provides that where any law requires any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form. (*Clause 4* of the Information Technology Bill, 1999)

S. 5. 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 affixed 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.

NOTES

This clause provides for legal recognition of Digital Signatures. It shall be authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government. (*Clause 5* of the Information Technology Bill, 1999)

S. 6. Use of electronic records and digital signatures in Government and its agencies

(1) Where any law provides for—

(*a*) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(*b*) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(*c*) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (*1*), by rules, prescribe—

(*a*) the manner and format in which such electronic records shall be filed, created or issued;

(*b*) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (*a*).

NOTES

This clause lays down the foundation of Electronic Governance. The filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. (*Clause 6* of the Information Technology Bill, 1999)

S. 7. 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—

(*a*) the information contained therein remains accessible so as to be usable for a subsequent reference;

(*b*) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(*c*) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

S. 8. Publication of rule, 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, buy-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of that Official Gazette which was first published in any form.

NOTES

This clause provides for the publication of rules, regulations and notifications in the Electronic Gazette. Where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter should be published in the Official Gazette, then such requirement shall be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form. (*Clause 8* of the Information Technology Bill, 1999)

S. 9. 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 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.

NOTES

This clause provides for the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist the document should be accepted in an electronic form by any Ministry or Department of the Central Government or the State Government. (*Clause 9* of the Information Technology Bill, 1999)

S. 10. Power to make rules by Central Government in respect of digital signature

The Central Government may, for the purposes of this Act, by rules, prescribe—

(*a*) the type of digital signature;

(*b*) the manner and format in which the digital signature shall be affixed;

(*c*) the manner or procedure which facilitates identification of the person affixing the digital signature;

(*d*) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(*e*) any other matter which is necessary to give legal effect to digital signatures.

NOTES

This clause provides for the power to make rules by the Central Government in respect of Digital Signature. (*Clause 10* of the Information Technology Bill, 1999)

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

S. 11. Attribution of electronic records

An electronic record shall be attributed to the originator—

(*a*) if it was sent by the originator himself;

(*b*) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(*c*) by an information system programmed by or on behalf of the originator to operate automatically.

NOTES

This clause deals with the attribution of the electronic records to the originator. (*Clause 11* of the Information Technology Bill, 1999)

S. 12. Acknowledgment of Receipt

(1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—

(*a*) any communication by the addressee, automated or otherwise; or

(*b*) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(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.

NOTES

This clause provides for the acknowledgment of receipt of an electronic record by various modes. (*Clause 12* of the Information Technology Bill, 1999)

S. 13. Time and place of dispatch 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 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,—

(*i*) receipt occurs at the time when the electronic record enters the designated computer resource; or

(*ii*) 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.

(3) Save as otherwise agreed 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.

(4) The provisions 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*).

(5) For the purposes of this section,—

(*a*) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(*b*) 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;

(*c*) "usual place of residence", in relation to a body corporate, means the place where it is registered.

NOTES

This clause provides for the time and place of despatch and receipt of electronic record sent by the originator. (*Clause 13* of the Information Technology Bill, 1999*)*

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

S. 14. 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.

NOTES

This clause provides for the security procedure which has to be applied to an electronic record for being treated as a secure electronic record. (*Clause 14* of the Information Technology Bill, 1999*)*

S. 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.

NOTES

This clause provides for the security procedure to be applied to Digital Signatures for being treated as a secure digital signature. (*Clause 15* of the Information Technology Bill, 1999)

S. 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.

NOTES

This clause provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. (*Clause 16* of the Information Technology Bill, 1999)

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

S. 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 superintendent 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.

NOTES

This clause provides for the appointment of Controller and other officers to regulate the Certifying Authorities. (*Clause 17* of the Information Technology Bill, 1999)

S. 18. Functions of Controller

The Controller may perform all or any of the following functions, namely:—

(*a*) exercising supervision over the activities of the Certifying Authorities;

(*b*) Certifying public keys of the Certifying Authorities;

(*c*) laying down the standards to be maintained by the Certifying Authorities;

(*d*) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(*e*) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(*f*) specifying the contents 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;

(*g*) specifying the form and content of a Digital Signature Certificate and the key;

(*h*) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(*i*) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(*j*) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(*k*) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(*l*) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(*m*) laying down the duties of the Certifying Authorities;

(*n*) maintaining a data-base containing of disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

NOTES

This clause provides for the functions of the Controller in respect of activities of Certifying Authorities which may be prescribed by regulations. (*Clause 18* of the Information Technology Bill, 1999)

S. 19. Recognition of foreign Certifying Authorities

(1) 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 Foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) 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.

(3) 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.

NOTES

This clause provides for the power of the Controller with the previous approval of the Central Government to grant recognition for foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. (*Clause 19* of the Information Technology Bill, 1999)

S. 20. Controller to act as repository

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(*a*) make use of hardware, software and procedures that are secure from instrusion and misuse;

(*b*) observe such other standards as may be prescribed by the Central Government,

to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data-base of all public keys in such a manner that such data-base and the public keys are available to any member of the public.

NOTES

This clause provides that the Controller shall be acting as repository of all Digital Signature Certificates issued under the Act. He shall also adhere to certain security procedure to ensure secrecy and privacy of the digital signatures and also to satisfy such other standards as may be prescribed by the Central Government. (*Clause 20* of the Information Technology Bill, 1999)

S. 21. Licence to issue Digital Signature Certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (7), unless the applicant fulfills such requirements 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.

(3) A licence granted under this section shall—

(*a*) be valid for such period as may be prescribed by the Central Government;

(*b*) not be transferable or heritable;

(*c*) be subject to such terms and conditions as may be specified by the regulations.

NOTES

This clause provides that a licence to be issued to a Certifying Authority to issue Digital Signature Certificates by the Controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application either grant the licence or reject the application after giving reasonable opportunity of being heard. (*Clause 21* of the Information Technology Bill, 1999)

S. 22. Application for Licence

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by—

(*a*) a certification practice statement;

(*b*) a statement including the procedures with respect to identification of the applicant;

(*c*) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(*d*) such other documents, as may be prescribed by the Central Government.

NOTES

This clause provides that the application for licence shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. (*Clause 22* of the Information Technology Bill, 1999)

S. 23. Renewal of Licence

An application for renewal of a licence shall be—

(*a*) in such form;

(*b*) accompanied by such fees, not exceeding five thousand rupees,

as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence:

Provided that an application for the renewal of the licence made after the expiry of the licence may be entertained on payment of such late fee, not exceeding five hundred rupees, as may be prescribed.

NOTES

This clause provides that the application for renewal of a licence shall be in such form and accompanied by such fees not exceeding five thousand rupees which may be prescribed by the Central Government. (*Clause 23* of the Information Technology Bill, 1999)

S. 24. Procedure for grant or rejection of Licence

The Controller may, on receipt of an application under sub-section (*1*) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence 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.

NOTES

This clause deals with the procedure for rejection of licence on certain grounds. (*Clause 24* of the Information Technology Bill, 1999)

S. 25. Suspension of Licence

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,—

(*a*) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(*b*) failed to comply with the terms and conditions subject to which the licence was granted;

(*c*) failed to maintain the standards specified under clause (*b*) of sub-section (*2*) of section 20;

(*d*) has contravened any provisions of this Act, rule, regulation or order made thereunder,

revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (*1*), by order suspend such licence pending the completion of any inquiry ordered by him:

Provided that no licence 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.

(3) No Certifying Authority whose license has been suspended shall issue any Digital Signature Certificate during such suspension.

NOTES

This clause provides for suspension of licence on the grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made thereunder. (*Clause 25* of the Information Technology Bill, 1999)

S. 26. Notice of suspension or revocation of licence

(1) Where the licence 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.

(2) 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 data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of data-base in such electronic or other media, as he may consider appropriate.

NOTES

This clause provides that the Controller shall publish a notice of suspension or revocation of licence as the case may be in the data base maintained by him. (*Clause 26* of the Information Technology Bill, 1999)

S. 27. 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.

NOTES

This clause provides that the Controller may in writing authorise the Deputy Controller, Assistant Controller or any officer to exercise any of his powers under the Act. (*Clause 27* of the Information Technology Bill, 1999)

S. 28. Power to investigate contraventions

(1) The 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.

(2) 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 (43 of 1961) and shall exercise such powers, subject to such limitations laid down under that Act.

NOTES

This clause provides that the Controller shall have power to investigate contraventions of the provisions of the Act or the rules or regulations made thereunder either by himself or through any officer authorised in *this* behalf. (*Clause 28* of the Information Technology Bill, 1999)

S. 29. Access to computers and data

(1) Without prejudice to the provisions of sub-section (*1*) of section 69, 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.

(2) For the purposes of sub-section (*1*), 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.

NOTES

This clause provides that the Controller or any person authorised by him, if lie has reasonable cause to suspect that contravention of the provisions of the Act or the rules or regulations is being committed, shall have access to any computer system, data or any other material connected with such system. (*Clause 29* of the Information Technology Bill, 1999)

S. 30. Certifying Authority to follow certain procedures

Every Certifying Authority shall—

(*a*) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(*b*) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(*c*) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(*d*) observe such other standards as may be specified by regulations.

NOTES

This clause provides for the Certifying Authority to follow certain procedure in respect of Digital Signatures. (*Clause 30* of the Information Technology Bill, 1999)

S. 31. 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.

NOTES

This clause provides that the Certifying Authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made thereunder. (*Clause 31* of the Information Technology Bill, 1999)

S. 32. Display of licence

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

NOTES

This clause provides that the Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. (*Clause 32* of the Information Technology Bill, 1999)

S. 33. Surrender of licence

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority facts to surrender a licence under sub-section (*1*), the person is whose favour a licence 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.

NOTES

This clause provides that the Certifying Authority whose licence is suspended or revoked shall immediately surrender the licence to the Controller. (*Clause 33* of the Information Technology Bill, 1999)

S. 34. Disclosure

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

(*a*) 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;

(*b*) any certification practice statement relevant thereto;

(*c*) notice of the revocation or suspension of its Certifying Authority certificate. if any; and

(*d*) 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.

(2) Where in the opinion of the Certifying Authority any event has occurred or any 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—

(*a*) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(*b*) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

NOTES

This clause provides that every Certifying Authority shall disclose its Digital Signature Certificate which contains public key corresponding to the private key used by that Certifying Authority and other relevant facts. (*Clause 34* of the Information Technology Bill, 1999)

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

S. 35. Certifying Authority to issue Digital Signature Certificate

(1) 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.

(2) 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.

(3) 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.

(4) 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 as 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—

(*a*) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(*b*) the applicant holds a private key, which is capable of creating a digital signature;

(c) 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.

NOTES

This clause deals with the form in which Digital Signature Certificate may be issued by a Certifying Authority. (*Clause 35* of the Information Technology Bill, 1999)

S. 36. Representations upon issuance of Digital Signature Certificate

A Certifying Authority while issuing a Digital Signature Certificate shall certify that—

(*a*) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(*b*) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(*c*) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(*d*) the subscriber's public key and private key constitute a functioning key pair;

(*e*) the information contained in the Digital Signature Certificate is accurate; and

(*f*) 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*).

NOTES

This clause provides for the Certifying Authority to certify while issuing a Digital Signature Certificate that it has complied with the provisions of the Act, the rules and regulations made thereunder and also with other conditions mentioned in the Digital Signature Certificate. (*Clause 36* of the Information Technology Bill, 1999*)*

S. 37. Suspension of Digital Signature Certificate

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,—

(*a*) on receipt of a request to that effect from —

(*i*) the subscriber listed in the Digital Signature Certificate; or

(*ii*) any person duly authorised to act on behalf of that subscriber;

(*b*) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) 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.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

NOTES

This clause provides for the suspension of Digital Signature Certificate under certain circumstances. Further, such certificate shall not be suspended for a period of exceeding 15 days unless the subscriber has been given an opportunity of being heard. (*Clause 37* of the Information Technology Bill, 1999*)*

S. 38. Revocation of Digital Signature Certificate

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—

(*a*) where the subscriber or any other person authorised by him makes a request to that effect; or

(*b*) upon the death of the subscriber; or

(*c*) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) 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*) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(*b*) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(*c*) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(*d*) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

NOTES

This clause provides for the revocation of Digital Signature Certificates under certain circumstances. Further, such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. (*Clause 38* of the Information Technology Bill, 1999)

S. 39. Notice of suspension or revocation

(1) 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.

(2) 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.

NOTES

This clause provides that the Certifying Authority shall publish the suspension or revocation of a Digital Signature Certificate in the depository. (*Clause 39* of the Information Technology Bill, 1999)

CHAPTER VIII

DUTIES OF SUBSCRIBERS

S. 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.

NOTES

This clause provides that the subscriber shall generate a key pair using a secure system. (*Clause 40* of the Information Technology Bill, 1999)

S. 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;

(*b*) 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;

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

NOTES

This clause provides for the circumstances under which a subscriber shall be deemed to have accepted a Digital Signature Certificate. (*Clause 41* of the Information Technology Bill, 1999)

S. 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 take 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 compromised.

NOTES

This clause provides that the subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. (*Clause 42* of the Information Technology Bill, 1999)

CHAPTER IX

PENALTIES AND ADJUDICATION

S. 43. 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,—

(*a*) accesses or secures access to such computer, computer system or computer network.

(*b*) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(*c*) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(*d*) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(*e*) disrupts or causes disruption of any computer, computer system or computer network;

(*f*) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

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

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

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(*i*) "computer contaminant" means any set of computer instructions that are designed—

(*a*) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(*b*) by any means to usurp the normal operation of the computer, computer system, or computer network;

(*ii*) "computer 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;

(*iii*) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(*iv*) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

NOTES

This clause provides penalty for damage caused to any computer, computer network etc. by introduction of computer virus, unauthorised access and other types of mischief. Any person who is found guilty of contravening this section is liable to pay damages by way of compensation not exceeding ten lakh rupees to the person affected thereby. (*Clause 43* of the Information Technology Bill, 1999)

S. 44. Penalty for failure to furnish information, return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to—

(*a*) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(*b*) file any return or furnish any information, books or other documents within the time specified therefor 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;

(*c*) 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.

NOTES

This clause provides penalty for failure to furnish information, returns, etc., which is required to be furnished by any person under the Act which may extend up to one lakh and fifty thousand rupees for each such failure. It further provides for if the failure continues, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues. (*Clause 44* of the Information Technology Bill, 1999)

S. 45. Residuary penalty

Whoever 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.

NOTES

This clause provides liability to pay a compensation not exceeding twenty-five thousand rupees by a person who contravenes any regulations made under the Act for which no liability has been separately provided under the Act to the person affected by such contravention. (*Clause 45* of the Information Technology Bill, 1999)

S. 46. 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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—

(*a*) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 (45 of 1860) of the Indian Penal Code;

(*b*) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

NOTES

This clause provides for the power to adjudicate contravention.; under the Act by an officer not below than the rank of a Director to the Government of India or an equivalent officer of a State Government and for holding an enquiry in the prescribed manner after giving reasonable opportunity of being heard. (*Clause 46* of the Information Technology Bill, 1999)

S. 47. 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—

(*a*) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(*b*) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

NOTES

This clause provides that while adjudicating the quantum of compensation, the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss caused to any person. (*Clause 47* of the Information Technology Bill, 1999)

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

S. 48. 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.

(2) 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.

NOTES

This clause provides for establishment of one or more Appellate Tribunals to be known as Cyber Regulations Appellate Tribunal. Further, the Central Government by notification specify the matters and places in relation to such Tribunal. (*Clause 48* of the Information Technology Bill, 1999)

Clause 48 of the Bill relates to the establishment of Cyber Regulations Appellate Tribunal and clause 52 relates to the salaries and allowances payable to and the other terms and conditions of service including pension, gratuity and other retirement benefits of the presiding officer of the Tribunal. Sub-clause (3) of clause 56 of the Bill provides for the salaries and allowances and other conditions of service of the officers and employees of the Cyber Regulation Appellate Tribunal. Sub-clause (4) of clause 87 of the Bill provides for such travelling and other allowances to be paid to the Members of the Committee.

2. It is assumed that the Bill, when enacted will involve a non-recurring expenditure of rupees seventy-five lakhs and recurring expenditure of rupees one hundred and fifty lakhs during every financial year.

3. The Bill does not involve any other non-recurring expenditure. (*Financial Memorandum* of the Information Technology Bill, 1999)

S. 49. 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.

NOTES

This clause provides for the Cyber Regulations Appellate Tribunal which shall consist of one person only who shall be appointed by notification by the Central Government. (*Clause 49* of the Information Technology Bill, 1999)

S. 50. 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—

(*a*) is, or has been, or is qualified to be, a Judge of a High Court; or

(*b*) 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.

NOTES

This clause provides for the qualifications for appointment as a Presiding Officer of the Tribunal. (*Clause 50* of the Information Technology Bill, 1999)

S. 51. 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.

NOTES

This clause provides that the Presiding Officer shall hold office subject to a maximum age limit of 65 years. (*Clause 51* of the Information Technology Bill, 1999)

S. 52. 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 service 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.

NOTES

This clause provides for the salary and allowances and other terms and conditions of service of the Presiding Officer. (*Clause 52* of the Information Technology Bill, 1999)

S. 53. 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 the stage at which the vacancy is filled.

NOTES

This clause provides for filling up of any vacancy occurring in the office of the Presiding Officer of Cyber Regulations Tribunal and also the procedure to be followed in case of a casual vacancy. (*Clause 53* of the Information Technology Bill, 1999)

S. 54. 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.

(2) 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.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

NOTES

This clause deals with the procedure for resignation or removal of the Presiding Officer. (*Clause 54* of the Information Technology Bill, 1999)

S. 55. 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.

NOTES

This clause provides that no order appointing any Presiding Officer shall be called in question merely on the ground of any defect in the constitution of the Tribunal. (*Clause 55* of the Information Technology Bill, 1999)

S. 56. Staff of the Cyber Appellate Tribunal

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) 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.

NOTES

This clause provides that the Central Government shall provide such officers for the functioning of the Cyber Regulations Appellate Tribunal. It empowers the Central Government to frame rules relating to salaries, allowances and other conditions of service of such officers and employees. (*Clause 56* of the Information Technology Bill, 1999)

S. 57. Appeal to Cyber Appellate Tribunal

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) 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 Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form 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.

(4) 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.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (*1*) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

NOTES

This clause provides for appeal by an aggrieved person against an order made by an adjudicating officer to the Cyber Appellate Tribunal. (*Clause 57* of the Information Technology Bill, 1999)

S. 58. Procedure and powers of the Cyber Appellate Tribunal

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:—

(*a*) summoning and enforcing the attendance of any person and examining him on oath;

(*b*) requiring the discovery and production of documents or other electronic records;

(*c*) receiving evidence on affidavits;

(*d*) issuing commissions for the examination of witnesses or documents;

(*e*) reviewing its decisions;

(*f*) dismissing an application for default or deciding it *ex parte;*

(g) any other matter which may be prescribed.

(3) 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 (2 of 1974).

NOTES

This clause provides for the procedure and powers of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the Civil Court under the Code of Civil Procedure, 1908. (*Clause 58* of the Information Technology Bill, 1999*)*

S. 59. 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.

NOTES

This clause provides that the appellant may either appear in person or may be represented by a legal practitioner to present his case before the Tribunal. (*Clause 59* of the Information Technology Bill, 1999*)*

S. 60. Limitation

The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

NOTES

This clause provides for period of limitation for admission of appeals from the aggrieved persons to the Cyber Appellate Tribunal. (*Clause 60* of the Information Technology Bill, 1999*)*

S. 61. 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.

NOTES

This clause provides that no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer has jurisdiction to determine. (*Clause 61* of the Information Technology Bill, 1999*)*

S. 62. 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.

NOTES

This clause provides for an appeal to the High Court by an aggrieved person from the decision of the Cyber Appellate Tribunal. (*Clause 62* of the Information Technology Bill, 1999)

S. 63. Compounding of contraventions

(1) 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.

(3) 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.

NOTES

This clause provides that any contravention under the Act shall be compounded by the Controller or adjudication officer either before or after the institution of the adjudication proceedings subject to such conditions he may impose. (*Clause 63* of the Information Technology Bill, 1999)

S. 64. 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 licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

NOTES

This clause provides for recovery of penalty as an arrears of land revenue and for suspension of the licence or Digital Signature Certificate till the penalty is paid. (*Clause 64* of the Information Technology Bill, 1999)

CHAPTER XI

OFFENCES

S. 65. 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.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer Commands, design and layout and programme analysis of computer resource in any form.

NOTES

This clause provides for punishment with imprisonment up to three years or with a fine which may extend to two lakh rupees or with both whoever knowingly or intentionally tampers with the computer source documents. (*Clause 65* of the Information Technology Bill, 1999)

S. 66. Hacking with computer system

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

S. 67. 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 five years and also with fine which may extend to two lakhs rupees.

NOTES

This clause provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to two years and with fine which may extend to twenty-five thousand rupees on first conviction and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to fifty thousand rupees. (*Clause 66* of the Information Technology Bill, 1999)

S. 68. Power of the Controller to give directions

(1) 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.

(2) Any person who fails to comply with any order under 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 fine not exceeding two lakh rupees or to both.

NOTES

This clause provides that the Controller may give directions to a Certifying Authority or any employee of such authority to take such measures or cease carrying such activities specified in such direction. (*Clause 67* of the Information Technology Bill, 1999)

S. 69. Directions of Controller to a subscriber to extend facilities to decrypt information

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or

public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (*1*), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

NOTES

This clause empowers the Controller, if he is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order to intercept any information transmitted through any computer system or computer net work. (*Clause 68* of the Information Technology Bill, 1999)

S. 70. Protected system

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (*1*).

(3) 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.

NOTES

This clause empowers the appropriate Governments by notification to declare any computer, computer system or computer network to be a protected system. Any unauthorised access of such systems will be punishable with imprisonment which may extend to ten years or with fine. (*Clause 69* of the Information Technology Bill, 1999)

S. 71. Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence 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.

NOTES

This clause provides that if any person misrepresenting or suppressing any material fact to the Controller or the Certifying Authority 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. (*Clause 70* of the Information Technology Bill, 1999)

S. 72. Penalty for 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 extend to one lakh rupees, or with both.

NOTES

This clause provides a punishment for breach of confidentiality and privacy with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both. (*Clause 71* of the Information Technology Bill, 1999)

S. 73. Penalty for publishing Digital Signature Certificate false in certain particulars

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(*a*) the Certifying Authority listed in the certificate has not issued it; or

(*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 created prior to such suspension or revocation.

(2) 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.

NOTES

This clause provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both. (*Clause 72* of the Information Technology Bill, 1999)

S. 74. Publication 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.

NOTES

This clause provides for 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 to a person whoever knowingly publishes for fraudulent purpose any Digital Signature Certificate. (*Clause 73* of the Information Technology Bill, 1999)

S. 75. Act to apply for offences or contravention committed outside India

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (*1*), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

NOTES

This clause provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. (*Clause 74* of the Information Technology Bill, 1999)

S. 76. 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 authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

NOTES

This clause provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules,, regulations or orders made thereunder. (*Clause 75* of the Information Technology Bill, 1999)

S. 77. Penalties or 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.

NOTES

This clause provides that penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force. (*Clause 76* of the Information Technology Bill, 1999)

S. 78. Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

NOTES

This clause provides for power to investigate the offences under the Act by a Police Officer not below than the rank of Deputy Superintendent of Police. (*Clause 77* of the Information Technology Bill, 1999)

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

S. 79. Network service providers not to 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 that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section,—

(*a*) "network service provider" means an intermediary;

(*b*) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

NOTES

This clause provides that the Network Service Providers not to be liable in certain circumstances. (*Clause 78* of the Information Technology Bill, 1999)

CHAPTER XIII

MISCELLANEOUS

S. 80. Power of police officer and other officers to enter, search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), 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 authorised 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.

(2) 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.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) 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.

NOTES

This clause empowers Police Officer not below the rank of Deputy Superintendent of Police or any other Officer of the Central or State Government to enter, search and seize and arrest any person who is reasonably suspected to have committed any offence under this Act. (*Clause 79* of the Information Technology Bill, 1999)

S. 81. 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.

NOTES

This clause provides that the provisions of the Act shall have overriding effect over the other law. (*Clause 80* of the Information Technology Bill, 1999)

S. 82. 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 45 of 1860.

NOTES

This clause provides that the Controller, Deputy Controller and Assistant Controller shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code. (*Clause 81* of the Information Technology Bill, 1999)

S. 83. 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.

NOTES

This clause provides for the Central Government to give directions to the Government of States as to the carrying into execution, the provisions of the Act. (*Clause 82* of the Information Technology Bill, 1999)

S. 84. Protection 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.

NOTES

This clause provides for protection of action taken in good faith by the Central Government, the State Government, the Controller or any person acting on behalf his under the Act. (*Clause 83* of the Information Technology Bill, 1999)

S. 85. Offences by companies

(1) 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 was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be 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.

(2) 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 thereunder 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.

Explanation,—For the purposes of this section,—

(*i*) "company" means any body corporate and includes a firm or other association of individuals; and

(*ii*) "director", in relation to a firm, means a partner in the firm.

NOTES

This clause provides for offences committed by companies. (*Clause 84* of the Information Technology Bill, 1999)

S. 86. Removal of difficulties

(1) 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.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

NOTES

This clause confers the power upon the Central Government to remove certain difficulties arising out of implementation of the provisions of the Act. (*Clause 85* of the Information Technology Bill, 1999)

Clause 85 of the Bill empowers the Central Government by order to remove certain difficulties which may appear to it to be necessary or expedient. Further such order shall not be made under this clause after the expiry of a period of two years from the commencement of this Act. Every

such order shall be laid before both Houses of Parliament. (*Memorandum Regarding Delegated Legislation* of the Information Technology Bill, 1999)

S. 87. Power of Central Government to make rules

(1) 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.

(2) 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:—

(*a*) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(*b*) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (*1*) of section 6;

(*c*) 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;

(*d*) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;

(*e*) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;

(*f*) the qualifications, experience and terms and conditions of service of controller, Deputy Controllers and Assistant Controllers under section 17;

(*g*) other standards to be observed by the Controller under clause (*b*) of sub-section (*2*) of section 20;

(*h*) the requirements which an applicant must fulfil under sub-section (*2*) of section 21;

(*i*) the period of validity of licence granted under clause (*a*) of sub-section (*3*) of section 21;

(*j*) the form in which an application for licence may be made under sub-section (*1*) of section 22;

(*k*) the amount of fees payable under clause (*c*) of sub-section (*2*) of section 22;

(*l*) such other documents which shall accompany an application for licence under clause (*d*) of sub-section (*2*) of section 22;

(*m*) the form and the fee for renewal of a licence and the fee payable thereof under section 23;

(*n*) the amount of late fee payable under the proviso to section 23;

(*o*) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (*1*) of section 35;

(*p*) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (*2*) of section 35;

(*q*) the manner in which the adjudicating officer shall hold inquiry under sub-section (*1*) of section 46;

(*r*) the qualification and experience which the adjudicating officer shall possess under sub-section (*2*) of section 46;

(*s*) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;

(*t*) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (*3*) of section 54;

(*u*) the salary and allowances and other conditions, of service of other officers and employees under sub-section (*3*) of section 56;

(*v*) the form in which appeal may be filed and the fee thereof under sub-section (*3*) of section 57;

(*w*) any other power of a civil court required to be prescribed under clause (*g*) of sub-section (*2*) of section 58; and

(*x*) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Central Government under clause (*1*) of sub-section (*4*) of section 1 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 or both Houses agree that 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 modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

NOTES

This clause confers power upon the Central Government to make rules. (*Clause 86* of the Information Technology Bill, 1999)

Clause 86 of the Bill empowers the Central Government to make rules by notification to carry out the provisions of the Act. The matters in respect of which such rules may be made are specified therein. These matters relate, *inter alia,* to the electronic form in which filing, creation, grant or payment shall be made, types of digital signatures, the security procedure for creating secure electronic record and secure digital signature, the conditions to be fulfilled by an applicant for granting licence, renewal and revocation of such licence, the manner in which the adjudicating officer shall hold inquiry, the salary, allowances and other terms and conditions of service of the presiding officer of the Cyber Appellate Tribunal, the procedure for investigation of misbehaviour or incapacity of the presiding officer, the form of appeal, the salary and allowances and other conditions of service of other officers and employees of the Tribunal. (*Memorandum Regarding Delegated Legislation* of the Information Technology Bill, 1999)

S. 88. Constitution of Advisory Committee

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise—

(*a*) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(*b*) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

NOTES

This clause provides for constitution of a Cyber Regulations Advisory Committee which may advise the Central Government on certain matters under the Act. (*Clause 87* of the Information Technology Bill, 1999)

S. 89. Power of Controller to make regulations

(1) 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.

(2) 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:—

(*a*) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (*m*) of section 18;

(*b*) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (*1*) of section 19;

(*c*) the terms and conditions subject to which a licence may be granted under clause (*c*) of sub-section (*3*) of section 21;

(*d*) other standards to be observed by a Certifying Authority under clause (*d*) of section 30;

(*e*) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (*1*) of section 34;

(*f*) the particulars of statement which shall accompany an application under sub-section (*3*) of section 35.

(*g*) the manner in which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (*2*) of section 42.

(3) 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 be 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.

NOTES

This clause provides for power to the Controller to make regulations under the Act. (*Clause 88* of the Information Technology Bill, 1999*)*

Clause 88 of the Bill empowers the Controller to make regulations after consultation with the Cyber Regulation Advisory Committee and with the previous approval of the Central Government to carry out the purposes of this Act. The matters in respect of which such regulations may be made are specified therein. These matters relate, *inter alia,* to the particulars relating to maintenance of database containing the disclosure record of every Certifying Authority, conditions and restrictions subject to which the Controller may recognise any Certifying Authority to issue Digital Signature Certificate in a country outside India, the terms and conditions subject to which a licence may be granted and other standards to be observed by a Certifying Authority. (*Memorandum Regarding Delegated Legislation* of the Information Technology Bill, 1999*)*

S. 90. Power of state Government to make rules

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) 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:—

(*a*) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (*1*) of section 6;

(*b*) 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.

(3) 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.

NOTES

This clause provides power to the State Government to make rules. (*Clause 89* of the Information Technology Bill, 1999)

Clause 89 of the Bill empowers the State Government to make rules by notification to carry out the provisions of the Act. The matters in respect of which such rules may be made are specified therein. These matters relate, *inter alia,* to the electronic form in which filing, creation, grant or payment shall be affected, and certain other matters specified in sub-section (2) of section 6. (*Memorandum Regarding Delegated Legislation* of the Information Technology Bill, 1999)

S. 91. Amendment of Act 45 of 1860

The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

NOTES

This clause provides for amendment of the Indian Penal Code. The Indian Penal Code provides for offences relating to documents. It is proposed to amend various sections so as to take care of offences relating to electronic records also Accordingly,—

(i) a new definition clause containing "electronic record" is inserted as section 29A;

(ii) sections 167, 172, 173, 175, 192, 204 and 463, being amended to include electronic record also;

(iii) section 464 is being amended to provide punishment for making a false document or false electronic records;

(iv) sections 466, 468, 469, 470, 476 and 477A are being amended to include "electronic record" also. (*Clause 90* of the Information Technology Bill, 1999)

S. 92. Amendment of Act 1 of 1872

The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

NOTES

This clause provides for amendment of the Indian Evidence Act, 1872. The amendments are being made to take care of admissibility of electronic records along with paper based documents. Other consequential amendments are also being made to take note of the provisions of the Information Technology Act, 1999. Salient features of the amendments are as follows:—

(i) in section 3, in the definition of "evidence" for "all documents produced for the inspection of the Court" the words "the contents of electronic records" is also proposed to be inserted;

(ii) after the definition of "India" the expressions "Certifying Authority", "Digital Signature", "Digital Signature Certificate", "electronic form", "electronic records" "information" and "subscriber" shall have the meanings assigned to them in the Information Technology Act, 1999;

(iii) after section 22, a new section 22A is being inserted to provide for relevance of oral admissions as to contents of electronic records in certain circumstances;

(iv) in sections 34 and 35, the words "electronic record" are also proposed to be added in addition to books of account and records;

(v) this clause seeks to substitute section 39 which provides for extent to which a statement forming part of a longer statement will be admissible in or take care of statement contained in electronic record;

(vi) after section 47, a new section 47A is proposed to be inserted in the Act in respect of opinion to be formed by the Court as to the digital signature by the Certifying Authority;

(vii) in section 59, the contents of "documents" is being substituted by contents of "documents or electronic records";

(viii) after section 65, two new sections namely, 65A and 65B are being proposed to be inserted which are special provision relating to electronic records and admissibility of computer outputs which is based on the lines sec 36A of the Central Excise Act, 1944 and section 138C of Custom Act, 1962;

(ix) after section 67, a new section 67A is proposed to be inserted providing for the circumstances in which the digital signature of a subscriber may be proved;

(x) after section 73, a new section 73A is proposed to be inserted to empower a court to direct a subscriber Certifying Authority or the Controller to produce a Digital Signature Certificate.

(xi) after section 81, a new section 81A is proposed to be inserted with reference to presumption as to the Official Gazette;

(xii) after section 85, three new sections 85A, 85B and 85C are proposed to be inserted with reference to presumptions as to electronic agreements, a electronic records, digital signatures and Digital Signature Certificate;

(xiii) after section 88, a new section 88A is proposed to be inserted in respect of presumptions as to electronic messages;

(xiv) after section 90, a new section 90A is proposed to be inserted in respect of presumptions as to electronic records five years old;

(xv) section 131 is proposed to be substituted for production of documents or electronic records which another person, having in his possession could refuse to produce. (*Clause 91* of the Information Technology Bill, 1999)

S. 93. 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.

NOTES

Provides for the amendment of the Banker's Book Evidence Act, 1891 as follows—

(i) to amend clauses (3) and (8) of section 2 which relates to definitions of "Banker's Book" and "certified copy".

(ii) after section 2, a new section 2A is proposed to be inserted imposing certain conditions in the print out. (*Clause 92* of the Information Technology Bill, 1999)

S. 94. 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.

NOTES

Provides for amendment of the Reserve Bank of India Act, 1934 to insert a new clause (*pp*) after clause (*p*) in sub-section (2) of section 58 with reference to the regulation of the fund transfer through electronic means. (*Clause 93* of the Information Technology Bill, 1999)

THE FIRST SCHEDULE

(*See* section 91)

AMENDMENTS TO THE INDIAN PENAL CODE

(45 of 1860)

Electronic record

1. After section 29, the following section shall be inserted, namely:—

"29A. The words "electronic record" shall have the meaning assigned to them in clause (*t*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.".

2. To section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall, be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 464,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", file following shall be substituted, namely:—

"A person is said to make a false document or false electronic record— First— Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature,

with the intention of causing it to be believed that such document or a part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly of fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after

it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.";

(b) after *Explanation* 2, the following *Explanation* shall be inserted at the end, namely:—

Explanation 3—For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause (*d*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.'

10. In section 466,—

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;

(b) the following *Explanation* shall be inserted at the end, namely:—

Explanation.—For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (*r*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.'

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely:—

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.".

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

THE SECOND SCHEDULE

(*See* section 92)

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872

(1 of 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", "elec-

tronic 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, 2000.'.

2. In section 17, for the words "oral or documentary,", the words "oral or documentary or contained in electronic format" shall be substituted.

When oral admission as to contents of electronic records are relevant

3. After section 22, the following section shall be inserted, namely:—

"22A. 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.

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

6. For section 39, the following section shall be substituted, namely:—

"39. 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 or 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.".

Opinion as to digital signature when relevant

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

"47A. 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.

Special provisions as to evidence relating to electronic record

9. After section 65, the following sections shall be inserted, namely:—

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

65B. (1) 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 (*1*) 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 computers, whether—

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

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

(*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 whatever 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 therefrom by calculation, comparison or any other process.'.

Proof as to digital signature

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

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged o have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

Proof as to verification of digital signatures

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

"73A. 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, 2000'.

Presumption as to Gazettes in electronic forms

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

"81A. 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.".

Presumption as to electronic agreements

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

"85A. 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.

Presumption as to electronic records and digital signatures

85B. (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.

Presumption as to Digital Signature Certificates

85C. 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."

Presumption as to electronic messages

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

'88A. The Court may presume 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 (*za*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.'.

Presumption as to electronic records five years old

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

"90A. 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 authorised 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.".

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

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

"131. No one shall be compelled to produce documents in his possession or electronic records under his 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 THIRD SCHEDULE

(*See* section 93)

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT, 1891

(18 of 1891)

1. In section 2—

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

'(3) "bankers' 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 a 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: and

(b) consist of printouts of data stored in an 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.'.

Conditions in the printout

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

"2A. 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; and

(*b*) a certificate by a person in-charge 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 unauthorised change of data;

(*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 electro-magnetic data storage devices:

(*E*) the mode of verification in order 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, the relevant data.".

THE FOURTH SCHEDULE

(*See* section 94)

AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934

(2 of 1934)

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (*p*), the following clause shall be inserted, namely:—

"(*pp*) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (*c*) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;".

ANNEXURE

EXTRACTS FROM THE INDIAN PENAL CODE

(45 of 1860)

Public servant framing an incorrect document with intent to cause injury

167. Whoever, being a public servant, and being, as such public servant, charged with the preparation or translation of any document, frames or translates that document in a manner which he

knows or believes to be incorrect, intending thereby to cause or knowing it to be likely that he may thereby cause injury to any person, shall be punished with imprisonment of either description for a term which may extend to three years or with fine or with both.

CHAPTER X

OF CONTEMPTS OF THE LAWFUL AUTHORITY OF PUBLIC SERVANTS

Absconding to avoid services of summons or other proceeding

172. Whoever absconds in order to avoid being served with a summons, notice or order proceeding from any public servant legally competent, as such public servant, to issue such summons, notice or order, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both;

or, if the summons or notice or order is to attend in person or by agent, or to produce a document in a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

Preventing service of summons or other proceeding, or preventing publication thereof

173. Whoever in any manner intentionally prevents the serving on himself, or on any other person, of any summons, notice or order proceeding from any public servant legally competent, as such public servant, to issue such summons, notice or order,

or intentionally prevents the lawful affixing to any place of any such summons, notice or order,

or intentionally removes any such summons, notice or order from any place to which it is lawfully affixed,

or intentionally prevents the lawful making of any proclamation, under the authority of any public servant legally competent, as such public servant, to direct such proclamation to be made,

shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both;

or, if summons, notice, order or proclamation is to attend in person or by agent, or to produce a document in a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

Omission to produce document to public servant by person legally bound to produce it

175. Whoever, being legally bound to produce or deliver up any document to any public servant, as such, intentionally omits so to produce or deliver up the same, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both;

or, if the document is to be produced or delivered up to a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

Illustration

A, being legally bound to produce a document before a District Court, intentionally omits to produce the same. A has committed the offence defined in this section.

Fabricating false evidence

192. Whoever causes any circumstance to exist or makes any false entry in any book or record, or makes any document containing a false statement, intending that such circumstance, false entry or false statement may appear in evidence in a judicial proceeding, or in a proceeding taken by law before a public servant as such, or before an arbitrator, and that such circumstance, false entry or false statement, so appearing in evidence, may cause any person who in such proceeding is to form an opinion upon the evidence, to entertain an erroneous opinion touching any point material to the result of such proceeding is said "to fabricate false evidence".

Illustrations

(a) A puts jewels into a box belonging to Z, with the intention that they may be found in that box, and that this circumstance may cause Z to be convicted of theft. A has fabricated false evidence.

(b) A makes a false entry in his shop-book for the purpose of using it as corroborative evidence in a Court of Justice. A has fabricated false evidence.

(c) A, with the intention of causing Z to be convicted of a criminal conspiracy, writes a letter in imitation of Z's handwriting, purporting to be addressed to an accomplice in such criminal conspiracy, and puts the letter in a place which he knows that the officers of the police are likely to search. A has fabricated false evidence.

Destruction of document to prevent its production as evidence

204. Whoever secrets or destroys any document which he may be lawfully compelled to produce as evidence in a Court of Justice, or in any proceeding lawfully held before a public servant, as such, or obliterates or renders illegible the whole or any part of such document with the intention of preventing the same from being produced or used as evidence before such Court or public servant as aforesaid, or after he shall have been lawfully summoned or required to produce the same for that purpose, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

CHAPTER XVIII

OF OFFENCES RELATING TO DOCUMENTS AND TO PROPERTY MARKS

Forgery

463. Whoever makes any false document or part of a document with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

Making a false document

464. A person is said to make a false document—

First.—Who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes any mark denoting the execution of a document, with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or

Secondly.—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document in any material part thereof, after it has been made or executed either by himself or by any other person, whether such person be living or dead at the time of such alteration ; or

Thirdly.—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document, knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration.

Illustrations

(a) A has a letter of credit upon Â for rupees 10,000, written by Z. A, in order to defraud B, adds a cipher to the 10,000, and makes the sum 1,00,000 intending that it may be believed by Â that Z so wrote the letter. A has committed forgery.

(b) A, without Z's authority, affixes Z's seal to a document purporting to be a conveyance of an estate from Z to A, with the intention of selling the estate to Â and thereby of obtaining from Â the purchase-money. A has committed forgery.

(c) A picks up a cheque on a banker signed by B, payable to bearer, but without any sum having been inserted in the cheque. A fraudulently fills up the cheque by inserting the sum of ten thousand rupees. A commits forgery.

(d) A leaves with B, his agent, a cheque on a banker, signed by A, without inserting the sum payable and authorizes B to fill up the cheque by inserting a sum not exceeding ten thousand rupees for the purpose of making certain payments. B fraudulently fills up the cheque by inserting the sum of twenty thousand rupees. B commits forgery.

(e) A draws a bill of exchange on himself in the name of B without B's authority, intending to discount it as a genuine bill with a banker and intending to take up the bill on its maturity. Here, as A draws the bill with intent to deceive the banker by leading him to suppose that he had the security of B, and thereby to discount the bill, A is guilty of forgery.

(f) Z's will contains these words-"I direct that all my remaining property be equally divided between A, B and C." A dishonestly scratches out B's name, intending that it may be believed that the whole was left to himself and C. A has committed forgery.

(g) A endorses a Government promissory note and makes it payable to Z or his order by writing on the bill the words "Pay to Z or his order" and signing the endorsement. B dishonestly erases the words "Pay to Z or his order", and thereby converts the special endorsement into a blank endorsement B commits forgery.

(h) A sells and conveys an estate to Z. A afterwards, in order to defraud Z of his estate, executes a conveyance of the same estate to B, dated six months earlier than the date of the conveyance to Z, intending it to be believed that be had-conveyed the estate to B before he conveyed it to Z. A has committed forgery.

(i) Z dictates his will to A. A intentionally writes down a different legatee from the legatee named by Z, and by representing to Z that he has prepared the will according to his instructions, induces Z to sign the will. A has committed forgery.

(j) A writes a letter and signs it with B's name without B's authority, certifying that A is a man of good character and in distressed circumstances from unforeseen misfortune, intending by means of such letter obtain alms from Z and other persons. Here, as A made a false document in order to induce Z to part with property, A has committed forgery.

(k) *A* without B's authority writes a letter and signs it in B's name certifying to A's character, intending thereby to obtain employment under Z. A has committed forgery in as much as he intended to deceive Z by the forged certificate, and thereby to induce Z to enter into an express or implied contract for service.

Explanation 1.—A man's signature of his own name may amount to forgery.

Illustrations

(a) *A* signs his own name to a bill of exchange, intending that it may be believed that the bill was drawn by another person of the same name. A has committed forgery.

(b) *A writes* the word "accepted" on a piece of paper and signs it with Z's name, in order that B may afterwards write on the paper a bill of exchange drawn by B upon Z, and negotiate me bill as though it had been accepted by Z. A is guilty of forgery; and if B, knowing the fact, draws the bill upon the paper pursuant to A's intention, B is also guilty of forgery.

(c) A picks up a bill of exchange payable to the order of a different person of the same name. A endorses the bill in his own name, intending to cause it to be believed that it was endorsed by the person to whose order it was payable, here A has committed forgery.

(d) *A* purchases an estate sold under execution of a decree against B. B, after the seizure of the estate, in collusion with Z, executes a lease of the estate, to Z at a nominal rent and for a long period and dates me lease six months prior to the seizure, with intent to defraud A, and to cause it to be believed that the lease was granted before the seizure. B, though he executes the lease in his own name, commits forgery by antedating it.

(e) A, a trader, in anticipation of insolvency, lodges effects with A for A's benefit, and with intent to defraud his creditors; and in order to give a colour to the transaction, writes a promissory note binding himself to pay to A a sum for value received, and antedates the note, intending that it

may be believed to have been made before A was on the point of insolvency. A has committed forgery under the first head of the definition.

Explanation 2.—The making of a false document in the name of a fictitious person, intending it to be believed that the document was made by a real person, or in the name of a deceased person, intending it to be believed that the document was made by the person in his lifetime, may amount to forgery.

Illustration

A draws a bill of exchange upon a fictitious person, and fraudulently accepts the bill in the name of such fictitious person with intent to negotiate it. A commits forgery.

Forgery of record of Court or of public register, etc.

466. Whoever forges a document, purporting to be a record or proceeding of or in a Court of Justice, or a register of birth, baptism, marriage or burial, or a register kept by a public servant as such, or a certificate or document purporting to be made by a public servant in his official capacity, or an authority to institute or defend a suit, or to take any proceedings therein, or to confess judgment, or a power of attorney, shall be punished with imprisonment to either description for a term which may extend to seven years, and shall also be liable to fine.

Forgery for purpose of cheating

468. Whoever commits forgery, intending that the document forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Forgery for purpose of harming reputation

469. Whoever commits forgery, intending that the document forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Forged document

470. A false document made wholly or in part by forgery is designated "a forged document".

Using as genuine a forged document

471. Whoever fradulently or dishonestly uses as genuine any document which he knows or has reason to believe to be a forged document, shall be punished in the same manner as if he had forged such document.

Falsification of accounts

477A. Whoever, being a clerk, officer or servant, or employed or acting in the capacity of a clerk, officer or servant, wilfully, and with intent to defraud, destroys, alters, mutilates or falsifies any book, paper, writing, valuable security or account which belongs to or is in the possession of his employer, or has been received by him for or on behalf of his employer, or wilfully, and with intent to defraud, makes or abets the making of any false entry in, or omits or alters or abets the omission or alteration of any material particular from or in, any such book, paper, writing, valuable security or account, shall be punished with imprisonment of either description for a term which may extend to seven years or with fine, or with both.

Explanation.—It shall be sufficient in any charge under this section to allege a general intent to defraud without naming any particular person intended to be defrauded or specifying any particular sum of money intended to be the subject of the fraud, or any particular day on which the offence was committed.

EXTRACTS FROM THE INDIAN EVIDENCE ACT, 1872 (1 of 1872)

Interpretation clause.

3. In this Act the following words and expressions are used in the following senses, unless a contrary intention appears from the context:—

"Evidence" means and includes—

(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry;

such statements are called oral evidence;

(2) all documents produced for the inspection of the Court; such documents are called documentary evidence.

STATEMENTS MADE UNDER SPECIAL CIRCUMSTANCES

Entries in books of account when relevant

34. Entries in books of account, regularly kept in the course of business, are relevant whenever they refer to a matter into which the Court has to inquire, but such statements shall not alone be sufficient evidence to charge any person with liability.

Illustration

A sues A for Rs. 1,000, and shows entries in his account books showing A to be indebted to him to this amount. The entries are relevant, but are not sufficient, without other evidence, to prove the debt.

Relevancy of entry in public record made in performance of duty

An entry in any public or other official book, register or record, stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in performance of a duty specially enjoined by the law of the country in which such book, register or record is kept, is itself a relevant fact.

CHAPTER IV—OF ORAL EVIDENCE 59

Proof of facts by oral evidence

59. All facts, except the contents of documents, may be proved by oral evidence.

Production of documents which another person, having possession, could refuse to produce

131. No one shall be compelled to produce documents in his possession, which any other person would be entitled to refuse to produce if they were in his possession, unless such last-mentioned person consents to their production.

EXTRACTS FROM THE BANKER'S BOOK EVIDENCE ACT, 1891
(18 of 1891)

Definitions.—2. In this Act, unless there is something repugnant in the subject or context,—

(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank:

Order of court to be construed to be order made by specified officer

8. In the application of sections 5, 6 and 7 to any investigation or inquiry referred to be sub-clause (*iii*) *of* clause (4) of section 2, the order of a court or a Judge referred to in the said sections shall be construed as referring to an order made by an officer of a rank not lower than the rank of a Superintendent of Police as may be specified in this behalf by the appropriate Government

Explanation.—In this section, "appropriate Government" means the Government by which the police officer or any other person conducting the investigation or inquiry is employed.

EXTRACT FROM THE RESERVE BANK OF INDIA ACT, 1934
(2 of 1934)

Power of the Central Board to make regulations

58. *(1)*

(2) In particular and without prejudice to the generality of the foregoing provision, such regulations may provide for all or any of the following matters, namely.

Contents of Volume 1

The Indian Evidence Act, 1872

Note : Part III— **Production and Effect on Evidence,** section 101, onwards continued in Volume 2.

ABBREVIATIONS

The Indian Law Reports (published under authority) Calcutta series, Bombay series, Madras series, Allahabad series, Patna series, Rangoon series, &c., up to the year 1936 have been cited thus: 63 C ; 60 B ;59 M ;58 A ;15 P ;14 R ;&c., &c. Form 1937 the citations are : 1937, 1 Cal./2 Cal. ; 1937, Bom. ; 1937 Mad. ; 1937 All. ; &c. From 1937 Rangoon Law Reports (published under authority) have been cited thus : 1937 Rang. ; 1938 Rang. &c.

The All India Reporter, Calcutta, Bombay, Madras, Allahabad, Rangoon, &c., &c., have been cited thus : A 1938 C ; A 1938 B ; A 1938 M ; A 1938 A ; A 1938 R ; &c.&c. The Privy Council and the Supreme Court parts have been cited thus: A 1938 PC ; A 1938 SC For Punjab (1) cases in the A.I.R. the former abbreviation EP has been continued. DR = Dacca Reports (CWN); SCR = Supreme Court Reports (Official).

Others explain themselves.