TO BE INTRODUCED IN LOK SABHA

Bill No. 96 of 2006

THE INFORMATION TECHNOLOGY (AMENDMENT) BILL, 2006

A

BILL

further to amend the Information Technology Act, 2000.

BE it enacted by Parliament in the Fifty-seventh Year of the Republic of India as follows:—

PART I

PRELIMINARY

Short title and commencement.

1. (*1*) This Act may be called the Information Technology (Amendment) Act, 2006.

(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint:

Provided that 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 coming into force of that provision.

PART II

AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000

Substitution of words "digital signature" by words "electronic signature".

2. In the Information Technology Act, 2000 (hereinafter in this Part referred to as the principal Act), for the words "digital signature" occurring in the Chapter, section, sub-section and clause referred to in the Table below, the words "electronic signature" shall be substituted. 21 of 2000.

TABLE

S.No.	Chapter/section/sub-section/clause
(1)	clauses (*d*), (*g*), (*h*) and (*zg*) of section 2;
(2)	section 5 and its marginal heading;
(3)	marginal heading of section 6;
(4)	clauses (*a*), (*b*), (*c*) and (*e*) of section 10 and its marginal heading;
(5)	heading of Chapter V;
(6)	clauses (*f*) and (*g*) of section 18;
(7)	sub-section (*2*) of section 19;
(8)	sub-sections (*1*) and (*2*) of section 21 and its marginal heading;
(9)	sub-section (*3*) of section 25;
(10)	clause (*c*) of section 30;
(11)	clauses (*a*) and (*d*) of sub-section (*1*) and sub-section (*2*) of section 34;
(12)	heading of Chapter VII;
(13)	section 35 and its marginal heading;
(14)	section 64;
(15)	section 71;
(16)	sub-section (*1*) of section 73 and its marginal heading;
(17)	section 74; and
(18)	clauses (*d*), (*n*) and (*o*) of sub-section (*2*) of section 87.

Amendment of section 1.

3. In section 1 of the principal Act, for sub-section (*4*), the following sub-sections shall be substituted, namely:—

"(*4*) Nothing in this Act shall apply to documents or transactions specified in the First Schedule:

Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.".

Amendment of section 2.

4. In section 2 of the principal Act,—

(*A*) for clause (*j*), the following clause shall be substituted, namely:—

'(*j*) "computer network" means the inter-connection of one or more computers or computer systems through—

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

(*ii*) terminals or a complex consisting of two or more inter-connected computers whether or not the inter-connection is continuously maintained;';

(*B*) in clause (*n*), the word "Regulations" shall be omitted;

(*C*) after clause (*n*), the following clause shall be inserted, namely:—

'(*na*) "cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;';

(*D*) after clause (*t*), the following clauses shall be inserted, namely:—

'(*ta*) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(*tb*) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;';

(*E*) in clause (*v*), for the words "data, text", the words "data, message, text" shall be substituted;

(*F*) for clause (*w*), the following clause shall be substituted, namely:—

'(*w*) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes, but does not include body corporate referred to in section 43A;'.

Amendment of heading of Chapter II.

5. In Chapter II of the principal Act, for the heading, the heading "DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE'' shall be substituted.

Insertion of new section 3A.

6. After section 3 of the principal Act, the following section shall be inserted, namely:—

Electronic signature.

"3A. (*1*) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (*2*), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which—

(*a*) is considered reliable; and

(*b*) may be specified in the Second Schedule.

(*2*) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(*a*) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(*b*) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(*c*) any alteration to the electronic signature made after affixing such signature is detectable;

(*d*) any alteration to the information made after its authentication by electronic signature is detectable; and

(*e*) it fulfils such other conditions which may be prescribed.

(*3*) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(*4*) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure

for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(*5*) Every notification issued under sub-section (*4*) shall be laid before each House of Parliament.".

Insertion of new section 6A.

7. After section 6 of the principal Act, the following section shall be inserted, namely:—

Delivery of services by service provider.

'6A. (*1*) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation.—For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(*2*) The appropriate Government may also authorise any service provider authorised under sub-section (*1*) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(*3*) Subject to the provisions of sub-section (*2*), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(*4*) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.'.

Insertion of new section 10A.

8. After section 10 of the principal Act, the following section shall be inserted, namely:—

Validity of contracts formed through electronic means.

"10A. Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.".

Amendment of section 12.

9. In section 12 of the principal Act, in sub-section (*1*), for the words "agreed with the addressee", the word "stipulated" shall be substituted.

Substitution of new sections for sections 15 and 16.

10. For sections 15 and 16 of the principal Act, the following sections shall be substituted, namely:—

Secure electronic signature.

'15. An electronic signature shall be deemed to be a secure electronic signature if—

(*i*) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(*ii*) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.—In case of digital signature, the "signature creation data" means the private key of the subscriber.

Security procedures and practices.

16. The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.'.

Omission of section 20.

11. Section 20 of the principal Act shall be omitted.

Amendment of section 29.

12. In section 29 of the principal Act, in sub-section (*1*), for the words "any contravention of the provisions of this Act, rules or regulations made thereunder", the words "any contravention of the provisions of this Chapter" shall be substituted.

Amendment of section 30.

13. In section 30 of the principal Act,—

(*i*) in clause (*c*), after the word "assured", the word "and" shall be omitted;

(*ii*) after clause (*c*), the following clauses shall be inserted, namely:—

"(*ca*) be the repository of all Electronic Signature Certificates issued under this Act;

(*cb*) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and".

Amendment of section 34.

14. In section 34 of the principal Act, in sub-section (*1*), in clause (*a*), the words "which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate" shall be omitted.

Amendment of section 35.

15. In section 35 of the principal Act, in sub-section (*4*), —

(*a*) the first proviso shall be omitted;

(*b*) in the second proviso, for the words "Provided further", the word "Provided" shall be substituted.

Amendment of section 36.

16. In section 36 of the principal Act, after clause (*c*), the following clauses shall be inserted, namely:—

"(*ca*) the subscriber holds a private key which is capable of creating a digital signature;

(*cb*) 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 subscriber;".

Insertion of new section 40A.

17. After section 40 of the principal Act, the following section shall be inserted, namely:—

Duties of subscriber of Electronic Signature Certificate.

"40A. In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.''.

Amendment of heading of Chapter IX.

18. In Chapter IX of the principal Act, in the heading, for the words "PENALTIES AND ADJUDICATION ", the words "PENALTIES, COMPENSATION AND ADJUDICATION" shall be substituted.

Amendment of section 43.

19. In section 43 of the principal Act,—

(*a*) in the marginal heading, for the word "Penalty", the word "Compensation" shall be substituted;

(*b*) after clause (*h*), the following clause shall be inserted, namely:—

"(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means,".

Insertion of new section 43A.

20. After section 43 of the principal Act, the following section shall be inserted, namely:—

Compensation for failure to protect data.

'43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Explanation.—For the purposes of this section,—

(*i*) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(*ii*) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(*iii*) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.'.

Amendment of section 46.

21. In section 46 of the principal Act, in sub-section (*1*), for the words "direction or order made thereunder", the words "direction or order made thereunder which renders him liable to pay penalty or compensation," shall be substituted.

Amendment of heading of Chapter X.

22. In Chapter X of the principal Act, in the heading, the word "REGULATIONS" shall be omitted.

Amendment of section 48.

23. In section 48 of the principal Act, in sub-section (*1*), the word "Regulations" shall be omitted.

Substitution of new sections for sections 49 to 52.

24. For sections 49 to 52 of the principal Act, the following sections shall be substituted, namely:—

Composition of Cyber Appellate Tribunal.

"49. (*1*) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint.

(*2*) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

(*3*) Subject to the provisions of this Act—

(*a*) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof;

(*b*) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two Members of such Tribunal as the Chairperson may deem fit:

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (*3*) of section 50;

(*c*) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with

the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify;

(*d*) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(*4*) Notwithstanding anything contained in sub-section (*3*), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench.

(*5*) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal.

50. (*1*) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court.

(*2*) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (*3*), shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs:

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two years or Joint Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than seven years.

(*3*) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five years.

Term of office, conditions of service, etc., of Chairperson and Members.

51. (*1*) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

(*2*) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(*3*) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member.

Salary, allowances and other terms and conditions of service of Chairperson and Members.

52. The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of the Cyber Appellate Tribunal shall be such as may be prescribed.

Powers of superintendence, direction, etc.

52A. The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

Distribution of business among Benches.

52B. Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

Power of Chairperson to transfer cases.

52C. On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or *suo motu* without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

Decision by majority.

52D. If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.".

Amendment of section 53.

25. In section 53 of the principal Act, for the words "Presiding Officer", the words "Chairperson or Member, as the case may be," shall be substituted.

Amendment of section 54.

26. In section 54 of the principal Act, for the words "Presiding Officer" wherever they occur, the words "Chairperson or the Member" shall be substituted.

Amendment of section 55.

27. In section 55 of the principal Act, for the words "Presiding Officer", the words "Chairperson or the Member" shall be substituted.

Amendment of section 56.

28. In section 56 of the Principal Act, for the words "Presiding Officer", the word "Chairperson" shall be substituted.

Amendment of section 61.

29. In section 61 of the principal Act, the following proviso shall be inserted at the end, namely:—

"Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter.".

Amendment of section 64.

30. In section 64 of the principal Act,—

(*i*) for the words "penalty imposed", the words "penalty imposed or compensation awarded" shall be substituted;

(*ii*) in the marginal heading, for the word "penalty", the words "penalty or compensation" shall be substituted.

Substitution of new sections for sections 66 and 67.

31. For sections 66 and 67 of the principal Act, the following sections shall be substituted, namely:—

Computer related offences.

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

Explanation.—For the purposes of this section,—

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

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

Punishment for sending offensive messages through communication service, etc.

66A. Any person who sends, by means of a computer resource or a communication device,—

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

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

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

Explanation.—For the purposes of this section, the term "communication device" means cell phones, personal digital assistance (PDA) or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

Punishment for publishing or transmitting obscene material in electronic form.

67. Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who 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 two years and with fine which may extend to five lakh rupees 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 ten lakh rupees.

Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

67A. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct 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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception.—This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form—

(*i*) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(*ii*) which is kept or used *bona fide* for religious purposes.'.

Amendment of section 68.

32. In section 68 of the principal Act, for sub-section (*2*), the following sub-section shall be substituted, namely:—

"(*2*) Any person who intentionally or knowingly 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 two years or a fine not exceeding one lakh rupees or both.".

Substitution of new section for section 69.

33. For section 69 of the principal Act, the following section shall be substituted, namely:—

Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

"69. (*1*) Where the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the Government to intercept or monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted through any computer resource.

(*2*) The Central Government shall prescribe safeguards subject to which such interception or monitoring or decryption may be made or done, as the case may be.

(*3*) The subscriber or intermediary 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—

(*a*) provide access to the computer resource containing such information;

(*b*) intercept or monitor or decrypt the information;

(*c*) provide information contained in computer resource.

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

Amendment of section 70.

34. In section 70 of the principal Act,—

(*a*) for sub-section (*1*), the following sub-section shall be substituted, namely:—

'(*1*) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.—For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.';

(*b*) after sub-section (*3*), the following sub-section shall be inserted, namely:—

"(*4*) The Central Government shall prescribe the information security practices and procedures for such protected system.".

Insertion of new section 70A.

35. After section 70 of the principal Act, the following section shall be inserted, namely:—

Indian Computer Emergency Response Team to serve as national nodal agency.

"70A. (*1*) The Indian Computer Emergency Response Team (CERT-In) shall serve as the national nodal agency in respect of Critical Information Infrastructure for co-ordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report.

(*2*) For the purposes of sub-section (*1*), the Director of the Indian Computer Emergency Response Team may call for information pertaining to cyber security from the service providers, intermediaries or any other person.

(*3*) Any person who fails to supply the information called for under sub-section (*2*), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(*4*) The Director of the Indian Computer Emergency Response Team may, by order, delegate his powers under this section to his one or more subordinate officers not below the rank of Deputy Secretary to the Government of India.".

Insertion of new section 72A.

36. After section 72 of the principal Act, the following section shall be inserted, namely:—

Punishment for disclosure of information in breach of lawful contract.

"72A. Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such 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 five lakh rupees, or with both.".

Substitution of new sections for sections 77 and 78.

37. For sections 77 and 78 of the principal Act, the following sections shall be substituted, namely:—

"77. No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

Compensation, penalties or confiscation not to interfere with other punishment.

77A. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, offences under sections 66, 66A, 72 and 72A may be compounded by the aggrieved person:

2 of 1974.

Offences under sections 66, 66A, 72 and 72A to be compoundable.

Provided that the provisions of this section does not apply where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind for such offence.

77B. No court shall take cognizance of an offence punishable under sections 66, 66A, 72 and 72A, except upon a complaint made by the person aggrieved by the offence.

Cognizance of offences under sections 66, 66A, 72 and 72A.

78. (*1*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, no police officer below the rank of Deputy Superintendent of Police shall investigate any cognizable offence under this Act.

2 of 1974.

Power to investigate offences.

(*2*) When information is given to an officer in charge of a police station of the commission within the limits of such station of a non-cognizable offence under this Act, he shall cause to be entered the substance of the information in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.

(*3*) Any police officer receiving such information may exercise the same powers in respect of investigation (except the power to arrest without warrant) as an officer in charge of the police station may exercise in a cognizable case under section 156 of the Code of Criminal Procedure, 1973.".

2 of 1974.

38. For Chapter XII of the principal Act, the following Chapters shall be substituted, namely:—

Substitution of new Chapters for Chapter XII.

'CHAPTER XII

INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. (*1*) Notwithstanding anything contained in any other law for the time being in force but subject to the provisions of sub-sections (*2*) and (*3*), an intermediary shall not be liable for any third party information, data, or communication link made available by him.

Exemption from liability of intermediary in certain cases.

(*2*) The provisions of sub-section (*1*) shall apply if—

(*a*) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(*b*) the intermediary does not—

(*i*) initiate the transmission,

(*ii*) select the receiver of the transmission, and

(*iii*) select or modify the information contained in the transmission.

(*3*) The provisions of sub-section (*1*) shall not apply if—

(*a*) the intermediary has conspired or abetted in the commission of the unlawful act;

(*b*) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary

fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

(*4*) Intermediary shall observe such other guidelines as the Central Government may prescribe in this behalf.

Explanation.—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

CHAPTER XIIA

EXAMINER OF ELECTRONIC EVIDENCE

Central Government to notify Examiner of Electronic Evidence.

79A. The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.—For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.'.

Omission of section 80.

39. Section 80 of the principal Act shall be omitted.

Amendment of section 81.

40. In section 81 of the principal Act, the following proviso shall be inserted at the end, namely:—

"Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970.". 14 of 1957. 39 of 1970.

Amendment of section 82.

41. In section 82 of the principal Act,—

(*a*) for the marginal heading, the following marginal heading shall be substituted, namely:—

"Chairperson, Members, officers and employees to be public servants.";

(*b*) for the words "Presiding Officer", the words "Chairperson, Members" shall be substituted.

Amendment of section 84.

42. In section 84 of the principal Act, for the words "Presiding Officer", the words "Chairperson, Members" shall be substituted.

Insertion of new sections 84A, 84B and 84C.

43. After section 84 of the principal Act, the following sections shall be inserted, namely:—

Modes or methods for encryption.

"84A. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

Punishment for abetment of offences.

84B. Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.—An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Punishment for attempt to commit offences.

84C. Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the

offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.".

Amendment of section 87.

44. In section 87 of the principal Act,—

(*A*) in sub-section (*2*),—

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

"(*a*) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (*2*) of section 3A;

(*aa*) the procedure for ascertaining electronic signature or authentication under sub-section (*3*) of section 3A;

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

(*ii*) after clause (*c*), the following clause shall be inserted, namely:—

"(*ca*) the manner in which the authorised service provider may collect, retain and appropriate service charges under sub-section (*2*) of section 6A;";

(*iii*) for clause (*e*), the following clauses shall be substituted, namely:—

"(*e*) the manner of storing and affixing electronic signature creation data under section 15;

(*ea*) the security procedures and practices under section 16;";

(*iv*) clause (*g*) shall be omitted;

(*v*) after clause (*m*), the following clause shall be inserted, namely:—

"(*ma*) the form of application and fee for issue of Electronic Signature Certificate under section 35;

(*vi*) after clause (*o*), the following clauses shall be inserted, namely:—

"(*oa*) the duties of subscribers under section 40A;

(*ob*) the reasonable security practices and procedures and sensitive personal data or information under section 43A;";

(*vii*) in clause (*r*), for the words "Presiding Officer", the words "Chairperson and Members" shall be substituted;

(*viii*) in clause (*s*), for the words "Presiding Officer", the words "Chairperson and Members" shall be substituted;

(*ix*) for clause (*w*), the following clauses shall be substituted, namely:—

"(*w*) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52A;

(*x*) the safeguards for interception or monitoring or decryption under sub-section (*2*) of section 69;

(*y*) the information security practices and procedures for protected system under section 70;

(*z*) the guidelines to be observed by the intermediaries under sub-section (*4*) of section 79;

(*za*) the modes or methods for encryption under section 84A;";

(*B*) in sub-section (*3*),—

(*i*) for the words, brackets, letter and figures "Every notification made by the Central Government under clause (*f*) of sub-section (*4*) of section 1 and every rule made by it", the words "Every rule made by the Central Government" shall be substituted;

(*ii*) the words "the notification or" wherever they occur, shall be omitted.

Amendment of section 90.

45. In section 90 of the principal Act, in sub-section (*2*), for clause (*c*), the following clause shall be substituted, namely:—

"(*c*) the form of information book under sub-section (*2*) of section 78.".

Omission of sections 91, 92, 93 and 94.

46. Sections 91, 92, 93 and 94 of the principal Act shall be omitted.

Substitution of new Schedules for First Schedule and Second Schedule.

47. For the First Schedule and the Second Schedule to the principal Act, the following Schedules shall be substituted, namely:—

"FIRST SCHEDULE

[*See* sub-section (*4*) of section 1]

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

Sl. No.	Description of documents or transactions	
1.	A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881.	26 of 1881.
2.	A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.	7 of 1882.
3.	A trust as defined in section 3 of the Indian Trusts Act, 1882.	2 of 1882.
4.	A will as defined in clause (*h*) of section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.	39 of 1925.
5.	Any contract for the sale or conveyance of immovable property or any interest in such property.	

THE SECOND SCHEDULE

[*See* sub-section (*1*) of section 3A]

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE

Sl. No.	Description	Procedure
(1)	(2)	(3)

.".

Omission of Third Schedule and Fourth Schedule.

48. The Third Schedule and the Fourth Schedule to the principal Act shall be omitted.

PART III

AMENDMENT OF THE INDIAN PENAL CODE

Amendment of Indian Penal Code.

49. In the Indian Penal Code— 45 of 1860.

Amendment of section 4.

(*a*) in section 4,—

(*i*) after clause (*2*), the following clause shall be inserted, namely:—

"(*3*) any person in any place without and beyond India committing offence targeting a computer resource located in India.";

(*ii*) for the *Explanation*, the following *Explanation* shall be substituted, namely:—

'*Explanation.*—In this section—

(*a*) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code;

(*b*) the expression "computer resource" shall have the meaning assigned to it in clause (*k*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.';

21 of 2000.

(*b*) in section 40, in clause (*2*), after the figure "117", the figures "118, 119 and 120" shall be inserted; Amendment of section 40.

(*c*) in section 118, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted; Amendment of section 118.

(*d*) in section 119, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted; Amendment of section 119.

(*e*) after section 417, the following section shall be inserted, namely:— Insertion of new section 417A.

"417A. Whoever, cheats by using the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to two years and shall also be liable to fine."; Punishment for identity theft.

(*f*) after section 419, the following section shall be inserted, namely:— Insertion of new section 419A.

"419A. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to five years and shall also be liable to fine. Punishment for cheating by personation using computer resource.

Explanation.—The expression "computer resource" shall have the meaning assigned to it in clause (*k*) of sub-section (*1*) of section 2 of the Information Technology Act, 2000.";

21 of 2000.

(*g*) in section 464 , for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted; Amendment of section 464.

(*h*) after Chapter XXI, the following Chapter shall be inserted, namely:— Insertion of new Chapter XXIA.

"CHAPTER XXIA

OF PRIVACY

502A. Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with simple imprisonment for a term which may extend to two years or with fine not exceeding two lakh rupees, or with both. Punishment for violation of privacy.

Explanation.—For the purpose of this section—

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

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

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

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

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

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

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

PART IV

AMENDMENT OF THE INDIAN EVIDENCE ACT, 1872

Amendment of Indian Evidence Act.

50. In the Indian Evidence Act, 1872,— 1 of 1872.

Amendment of section 3.

(*a*) in section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words "digital signature" and "Digital Signature Certificate", the words "electronic signature" and "Electronic Signature Certificate" shall respectively be substituted;

Insertion of new section 45A.

(*b*) after section 45, the following section shall be inserted, namely:—

Opinion of Examiner of Electronic Evidence.

"45A. When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact. 21 of 2000.

Explanation.—For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.";

Amendment of section 47A.

(*c*) in section 47A,—

(*i*) for the words "digital signature", the words "electronic signature" shall be substituted;

(*ii*) for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

Amendment of section 67A.

(*d*) in section 67A, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

Amendment of section 85A.

(*e*) in section 85A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted;

Amendment of section 85B.

(*f*) in section 85B, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

Amendment of section 85C.

(*g*) in section 85C, for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

Amendment of section 90A.

(*h*) in section 90A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted;

PART V

AMENDMENT OF THE CODE OF CRIMINAL PROCEDURE, 1973

2 of 1974.

51. In the Code of Criminal Procedure, 1973,— Amendment of Code of Criminal Procedure.

(*a*) after section 198A, the following section shall be inserted, namely:— Insertion of new section 198B.

"198B. No court shall take cognizance of an offence punishable under sections 417A, 419A and 502A of the Indian Penal Code, except upon a complaint made by the person aggrieved by the offence."; Prosecution of offences under sections 417A, 419A and 502A of Indian Penal Code.

45 of 1860.

(b) in section 320,— Amendment of section 320.

(*i*) in sub-section (*1*), in the Table, after the entries relating to—

(*A*) sections 352, 355 and 358, the following entries shall be inserted, namely:—

1	2	3
"Identity theft	417A	The person against whom the offence was committed.";

(*B*) section 502, the following entries shall be inserted, namely:—

1	2	3
"Violation of privacy	502A	The person against whom the offence was committed.";

(*ii*) in sub-section (*2*), in the Table, after the entries relating to section 419, the following entries shall be inserted, namely:—

1	2	3
"Cheating by personation by using computer resource	419A	The person against whom the offence was committed.";

(*iii*) in the First Schedule, under the heading "I. OFFENCES UNDER THE INDIAN PENAL CODE",—

(*A*) after the entries relating to section 417, the following entries shall be inserted, namely:—

1	2	3	4	5	6
"417A	Identity theft	Imprisonment for 2 years and fine.	Non-cognizable	Bailable	Any magistrate.";

(*B*) after the entries relating to section 419, the following entries shall be inserted, namely:—

1	2	3	4	5	6
"419A	Cheating by personation by using computer resource	Imprisonment for 5 years and fine.	Cognizable	Bailable	Any magistrate.";

(*C*) after the entries relating to section 502, the following entries shall be inserted, namely:—

1	2	3	4	5	6
"502A	Violation of privacy	Imprisonment for 2 years or fine or both.	Non-cognizable	Bailable	Any magistrate.".

STATEMENT OF OBJECTS AND REASONS

The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

2. With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonisation with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system so as to restrict its access.

3. A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.

4. The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that all States accord favourable consideration to the said Model Law on Electronic Signatures. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonisation with the said Model Law.

5. The service providers may be authorised by the Central Government or the State Goverment to set up, maintain and upgrade the computerised facilities and also collect, retain and appropriate service charges for providing such services at such scale as may be specified by the Central Government or the State Government.

6. The Bill seeks to achieve the above objects.

NEW DELHI; DAYANIDHI MARAN.

The 6*th December*, 2006.

Notes on clauses

Clause 2.—This clause seeks to substitute the words "digital signatures" by the words "electronic signatures" as provided in the Table thereunder so as to make it technology neutral.

Clause 3.—This clause seeks to amend sub-section (*4*) of section 1 so as to exclude Negotiable Instruments, power of attorney, trust, will and contract from the application of the Act and to empower the Central Government to amend the entries in the First Schedule.

Clause 4.—This clause seeks to amend section 2 and to define certain new expressions.

Clause 5.—This clause seeks to substitute heading of Chapter II with new heading 'DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE' so as to make the Act technology neutral.

Clause 6.—This clause seeks to insert a new section 3A which provides for authentication of electronic record by electronic signature or electronic authentication technique. It also empowers the Central Government to insert in the Second Schedule any electronic signature or electronic authentication technique and prescribe the procedure for the purpose of ascertaining the authenticity of electronic signature.

Clause 7.—This clause seeks to insert a new section 6A which empowers the Central Government as well as the State Government to authorise the service providers for providing efficient services through electronic means to the public against appropriate service charges. Further the said section empowers the Central Government as well as the State Government to specify the scale of service charges.

Clause 8.—This clause seeks to insert a new section 10A to provide for contracts formed through electronic means.

Clause 9.—This clause seeks to make amendment in sub-section (*1*) of section 12 which is of a consequential nature.

Clause 10.—This clause seeks to substitute sections 15 and 16 so as to remove certain inconsistencies in the procedures relating to secure electronic signatures and to provide for security procedures and practices.

Clause 11.—This clause provides for omission of section 20 with a view to empower the Certifying Authority under section 30 to act as repository of electronic signatures.

Clause 12.—This clause seeks to make amendment in sub-section (*1*) of section 29 with a view to limit the powers of the Controller in respect of access to any computer system only with reference to the provisions of Chapter VI and not with reference to the provisions of entire Act. The powers with respect to access to any computer system under other provisions of the Act are proposed to be entrusted to the Central Government under section 69.

Clause 13.—This clause seeks to amend section 30 with a view to empower the Certifying Authority to be the repository of all Electronic Signature Certificates issued under the Act.

Clause 14.—This clause seeks to amend section 34 with a view to make the provisions of that section technology neutral.

Clause 15.—This clause seeks to amend section 35 with a view to omit the first proviso to sub-section (*4*) so as to make the provisions of that section technology neutral.

Clause 16.—This clause seeks to amend section 36 so as to add two more representations for issuance of digital signature.

Clause 17.—This clause seeks to insert a new section 40A which provides for duties of the subscriber of Electronic Signature Certificate.

Clause 18.—This clause seeks to make an amendment in the Chapter heading of Chapter IX with a view to provide for making compensation for damages in respect of various contraventions.

Clause 19.—This clause seeks to amend section 43 so as to add certain more contraventions for damaging computer or computer system.

Clause 20.—This clause seeks to insert a new section 43A so as to empower the Central Goverment to provide for reasonable security practices and procedures and the sensitive personal data or information and also to provide for compensation for failure to protect sensitive personal data or information stored in a computer resource.

Clause 21.—This clause seeks to make amendment in section 46 with a view to make consequential changes.

Clauses 22 and 23.—These clauses seek to make amendments in the heading of Chapter X and section 48 with a view to suitably modify the same with the title of the Cyber Appellate Tribunal as mentioned in clause (*n*) of sub-section (*1*) of section 2.

Clause 24.—This clause seeks to substitute sections 49 to 52 and insert new sections 52A to 52D. Section 49 provides for the establishment of the Cyber Appellate Tribunal. Sections 50, 51 and 52 provide for qualifications, term of office, conditions of service and salary and allowances of the Chairperson and Members of the said Tribunal. Sections 52A to 52 D provide for powers of the Chairperson and distribution of business among the Benches.

Clauses 25 to 28.—These clauses seek to make amendments in sections 53 to 56 with a view to make the Cyber Appellate Tribunal a multi-member body.

Clause 29.—This clause seeks to insert a proviso in section 61 so as to provide jurisdiction to courts in certain cases.

Clause 30.—This clause seeks to amend section 64 so as to recover the compensation also as the arrears of land revenue.

Clause 31.—This clause seeks to substitute sections 66 and 67 and insert new sections 66A and 67A with a view to make certain more computer related wrong actions punishable and enhance the penalty.

Clause 32.—This clause seeks to amend section 68 so as to reduce the quantum of punishment and fine.

Clause 33.—This clause seeks to substitute section 69 so as to empower the Central Government to issue directions to an agency for interception or monitoring or decryption of any information transmitted through any computer resource. It also provides for punishment for rendering assistance to such agency.

Clause 34.—This clause seeks to amend section 70 so as to enable the Central Government as well as the State Government to declare any computer resource as protected system. It also provides for information security practices and procedures for such protected system.

Clause 35.—This clause seeks to insert a new section 70A for empowering Indian Computer Emergency Response Team to serve as a national nodal agency in respect of Critical Information Infrastructure.

Clause 36.—This clause seeks to insert a new section 72A which makes the disclosure of information in breach of a lawful contract punishable.

Clause 37.—This clause seeks to substitute sections 77 and 78 and to insert new sections 77A and 77B. Section 77 provides that compensation, penalties or confiscation under the Act shall not interfere with the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Section 77A provides for certain offences relating to computer resources as compoundable offences. Section 77B provides that Court shall take cognizance only on a complaint and not otherwise. Section 78 provides for power to investigate offences.

Clause 38.—This clause seeks to substitute Chapter XII and to insert a new Chapter XIIA which provides for exemption of intermediaries from liability in certain circumstances and also empowers the Central Government to prescribe guidelines to be observed by intermediaries for providing services. It also empowers the Central Government to specify the Examiner of Electronic Evidence.

Clause 39.—This clause seeks to omit section 80 of the Act with a view to entrust the powers of search and seizure, etc., to a Police Officer not below the rank of Deputy Superintendent of Police and for that purpose necessary provisions have been included in section 78 by substituting the same *vide* clause 37.

Clause 40.— This clause proposes to insert a proviso to section 81 so that the rights conferred under this section shall be supplementary to and not in derogation of the provisions of the Copyright Act or the Patents Act.

Clause 41.—This clause seeks to make amendment in section 82 with a view to declare the Chairperson, Members, officers and employees as public servants.

Clause 42.—This clause seeks to amend section 84 with a view to make consequential changes.

Clause 43.—This clause seeks to insert three new sections 84A, 84B and 84C with a view to empower the Central Government to prescribe the modes and methods of encryption for secure use of electronic media and for promotion of e-governance and e-commerce applications. Further it provides that abetment of and attempt to commit any offence shall also be punishable.

Clauses 44 and 45.—These clauses seek to make amendments in sections 87 and 90 respectively, which are of consequential nature.

Clause 46.—This clause seeks to omit sections 91 to 94 for the reason that these provisions have become redundant as necessary modifications have already been carried out in the Indian Penal Code and other related enactments.

Clause 47.—This clause seeks to substitute new Schedules for the First Schedule and the Second Schedule so as to provide for documents or transactions to which the provisions of the Act shall not apply. It also enables the list of electronic signature or electronic authentication technique and procedure for affixing such signature to be specified in the Second Scheudule.

Clause 48.—This clause seeks to omit the Third Schedule and Fourth Schedule as consequential to the omission of provisions of sections 93 and 94.

Clause 49.—This clause provides for certain amendments in the Indian Penal Code so as to specify certain offences relating to the computer resource.

Clause 50.—This clause provides for certain consequential amendments in the Indian Evidence Act pursuant to the changes proposed in the Act.

Clause 51.—This clause provides for amendments in the Code of Criminal Procedure by inserting new section 198B and amending section 320 so as to make certain consequential amendments pursuant to the changes proposed in the Act.

FINANCIAL MEMDORANDUM

Clause 24 of the Bill seeks to provide for multi-member composition of the Cyber Appellate Tribunal but the number of Members may be determined by the Central Government in the times to come. The salary, allowances and retirement benefits payable to the Chairperson and other Members of the Cyber Appellate Tribunal as and when appointed shall be met out of the annual Budget estimates of the Ministry. For the present, the Bill does not involve any additional recurring or non-recurring expenditure out of the Consolidated Fund of India.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 3 of the Bill seeks to amend sub-section (*4*) of section 1 which empowers the Central Government to amend the First Schedule by adding or deleting entries relating to documents or transactions to which the provisions of the Act shall not apply.

2. Clause 6 of the Bill seeks to insert a new section 3A *vide* which the Central Government is being empowered to—

(*a*) prescribe the conditions to be fulfilled for considering any electronic signature or electronic authentication technique as reliable;

(*b*) prescribe the procedure for affixing and authentication of electronic signature; and

(*c*) insert in the Second Schedule any electronic signature or electronic authentication technique and the procedure for affixing such signatures.

3. Clause 7 of the Bill seeks to insert a new section 6A which empowers the Central Government as well as the State Government to authorise the service provider to collect, retain and appropriate service charges. Further the said section empowers the Central Government and the State Government to specify, by notification, the scale of service charges.

4. Clause 10 of the Bill seeks to amend section 15 which empowers the Central Government to prescribe the manner of storing and affixing the signature creation data for a secure electronic signature. The said clause also seeks to amend section 16 which empowers the Central Government to prescribe the security procedures and practices for a secure electronic record and a secure electronic signature.

5. Clause 17 of the Bill seeks to insert a new section 40A which empowers the Central Government to prescribe the duties to be performed by the subscriber of the Electronic Signature Certificate.

6. Clause 20 of the Bill seeks to insert a new section 43A which empowers the Central Government to prescribe, in consultation with professional bodies or associations, the reasonable security practices and procedures and the sensitive personal data or information.

7. Clause 24 of the Bill seeks to substitute section 49 which empowers the Central Government to specify by notification the places for sitting of the Cyber Appellate Tribunal and the areas of their jurisdiction. Further, the said clause seeks to insert a new section 52A which empowers the Central Government to prescribe powers and functions of the Chairperson of the Cyber Appellate Tribunal.

8. Clause 33 of the Bill seeks to amend section 69 which empowers the Central Government to prescribe the safeguards for interception or monitoring or decryption.

9. Clause 34 of the Bill seeks to substitute sub-section (*1*) of section 70 which empowers the Central Government as well as the State Government to declare by notification any computer resource which affects the facility of Critical Information Infrastructure to be a protected system. Further, the said clause seeks to insert a new sub-section (*4*) to section 70 which empowers the Central Government to prescribe the information security practices and procedures for the protected system.

10. Clause 37 of the Bill seeks to substitute section 78 which empowers the State Government to prescribe the form of information book.

11. Clause 38 of the Bill seeks to substitute section 79. Sub-section (*4*) of the said section empowers the Central Government to prescribe the guidelines to be observed by

intermediary. Further, the said clause seeks to insert another new section 79A which empowers the Central Government to specify by notification the Examiner of Electronic Evidence for providing expert opinion on electronic form evidence.

12. Clause 42 of the Bill seeks to insert a new section 84A which empowers the Central Government to prescribe the modes and methods for encryption.

13. The matters in respect of which the said rules may be made or notification issued are matters of procedure and administrative detail, and as such, it is not practicable to provide for them in the proposed Bill itself.

14. The delegation of legislative power is, therefore, of a normal character.

ANNEXURE

EXTRACTS FROM THE INDIAN PENAL CODE

(45 OF 1860)

* * * * *

Extension of Code to extraterritorial offences.

4. The provisions of this Code apply also to any offence committed by—

* * * * *

(*2*) any person on any ship or aircraft registered in India wherever it may be.

Explanation.—In this section the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code.

Illustration

A, who is a citizen of India, commits a murder in Uganda. He can be tried and convicted of murder in any place in India in which he may be found.

* * * * *

"Offence".

40. Except in the Chapters and sections mentioned in clauses 2 and 3 of this section, the word "offence" denotes a thing made punishable by this Code.

In Chapter IV, Chapter VA and in the following sections, namely sections 64, 65, 66, 67, 71, 109, 110, 112, 114, 115, 116, 117, 187, 194, 195, 203, 211, 213, 214, 221, 222, 223, 224,225, 327, 328, 329, 330, 331, 347, 348, 388, 389 and 445, the word "offence" denotes a thing punishable under this Code, or under any special or local law as hereinafter defined.

And in sections 141, 176, 177, 201, 202, 212, 216 and 441, the word "offence" has the same meaning when the thing punishable under the special or local law is punishable under such law with imprisonment for a term of six months or upwards, whether with or without fine.

* * * * *

Concealing design to commit offence punishable with death or imprisonment for life—

118. Whoever intending to facilitate or knowing it to be likely that he will thereby facilitate the commission of an offence punishable with death or imprisonment for life.

voluntarily conceals, by any act or illegal omission, the existence of a design to commit such offence or makes any representation which he knows to be false respecting such design,

if offence be committed; if offence be not committed.

shall, if that offence be committed, be punished with imprisonment of either description for a term which may extend to seven years, or, if the offence be not committed, with imprisonment of either description, for a term which may extend to three years; and in either case shall also be liable to fine.

Illustration

A, knowing that dacoity is about to be committed at B, falsely informs the Magistrate that a dacoity is about to be committed at C, a place in an opposite direction, and thereby misleads the Magistrate with intent to facilitate the commission of the offence. The dacoity is committed at B in pursuance of the design. A is punishable under this section.

Public servant concealing design to commit offence which it is his duty to prevent—

119. Whoever, being a public servant intending to facilitate or knowing it to be likely that he will thereby facilitate the commission of an offence which it is his duty as such public servant to prevent.

voluntarily conceals, by any act or illegal omission, the existence of a design to commit such offence, or makes any representation which he knows to be false respecting such design,

shall, if the offence be committed. be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of such imprisonment, or with such fine as is provided for that offence, or with both; if offence be committed;

or, if the offence be punishable with death or imprisonment for life, with imprisonment of either description for a term which may extend to ten years; if offence be punishable with death, etc.;

or, if the offence be not committed, shall be punished with imprisonment of any description provided for the offence for a term which may extend to one-fourth part of the longest term of such imprisonment or with such fine as is provided for the offence, or with both. if offence be not committed,

Illustration

A. an officer of police, being legally bound to give information of all designs to commit robbery which may come to his knowledge, and knowing that B designs to commit robbery, omits to give such information, with intent to facilitate the commission of that offence. Here a has by an illegal omission concealed the existence of B's design and is liable to punishment according to the provision of this section.

* * * * *

464. A person is said to make a false document or false electronic record— Making a false document.

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 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 or 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.

Illustrations

(*a*) A has a letter of credit upon B 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 B 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 B and thereby of obtaining from B 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 he 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 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 to 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 inasmuch 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 the bills 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 the 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 B 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 B 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 fictious person, intending it to be believed that the document was made by 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.

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. 21 of 2000.

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.

* * * * *

———————

EXTRACTS FROM THE INDIAN EVIDENCE ACT, 1872

(1 OF 1872)

* * * * *

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

"Court" includes all Judges and Magistrates, and all persons, except arbitrators, legally authorised to take evidence. "Court".

"Fact" means and includes— "Fact".

(*1*) anything, state of things, or relation of things, capable of being perceived by the senses;

(*2*) any mental condition of which any person is conscious.

Illustrations

(*a*) That there are certain objects arranged in a certain order in a certain place, is a fact.

(*b*) That a man heard or saw something, is a fact.

(*c*) That a man said certain words, is a fact.

(*d*) That a man holds a certain opinion, has a certain intention, acts in good faith or fraudulently, or uses a particular word in a particular sense, or is or was at a specified time conscious of a particular sensation, is a fact.

(*e*) That a man has a certain reputation, is a fact.

One fact is said to be relevant to another when the one is connected with the other in any of the ways referred to in the provisions of this Act relating to the relevancy of facts. "Relevant".

The expression "facts in issue" means and includes— "Facts in issue".

any fact from which, either by itself or in connection with other facts, the existence, non-existence, nature or extent of any right, liability, or disability, asserted or denied in any suit or proceeding, necessarily follows.

Explanation.—Whenever, under the provisions of the law for the time being in force relating to Civil Procedure, any Court records an issue of fact, the fact to be asserted or denied in the answer to such issue is a fact in issue.

Illustrations

A is accused of the murder of B.

At his trial the following facts may be in issue:—

that A caused B's death;

that A intended to cause B's death;

that A had received grave and sudden provocation from B;

that A, at the time of doing the act which caused B's death, was, by reason of unsoundness of mind, incapable of knowing its nature.

"Document". "Document" means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.

Illustrations

A writing is a document:

Words printed lithographed or photographed are documents:

A map or plan is a document:

An inscription on a metal plate or stone is a document:

A caricature is a document.

"Evidence". "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 including electronic records produced for the inspection of the Court;

such documents are called documentary evidence.

"Proved". A fact is said to be proved when, after considering the matters before it, the Court either believes it to exist, or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists.

"Disproved". A fact is said to be disproved when, after considering the matters before it, the Court either believes that it does not exist, or considers its non-existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it does not exist.

"Not proved". A fact is said not to be proved when it is neither proved nor disproved.

"India". "India" means the territory of India excluding the State of Jammu and Kashmir.

the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000. 20 of 2000.

* * * * *

Opinion as to digital signature when relevant. **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.

* * * * *

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

* * * * *

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 agreements.

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. Presumption as to electronic records and digital signatures.

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

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

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

85C. 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 Digital Signature Certificates.

* * * * *

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. Presumption as to electronic records five years old.

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.

* * * * *

———

EXTRACTS FROM THE INFORMATION TECHNOLOGY ACT, 2000

(21 OF 2000)

* * * * *

CHAPTER I

PRELIMINARY

1. (*1*) * * * * * Short title, extent, commencement and application.

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

(*a*) a negotiable instrument (other than a cheque) 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 1882.

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

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

(*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.

Definitions.

2. (*1*) In this Act, unless the context otherwise requires,—

* * * * *

(*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;

* * * * *

(*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;

* * * * *

(*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;

* * * * *

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

* * * * *

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

(*w*) "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;

* * * * *

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

* * * * *

CHAPTER II

DIGITAL SIGNATURE

* * * * *

Legal recognition of digital signatures.

5. Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall 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.

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

6. (*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*).

* * * * *

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

10. 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.

* * * * *

Acknowledgement of receipt.

12. (*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.

* * * * *

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

* * * * *

Secure digital signature.

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

(*a*) unique to the subscriber affixing it;

(*b*) capable of identifying such subscriber;

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

then such digital signature shall be deemed to be a secure digital signature.

Security procedure.

16. 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.

* * * * *

Functions of Controller.

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

* * * * *

(*f*) specifying the contents of written, printed or visual materials 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;

* * * * *

Recognition of foreign Certifying Authorities.

19. (*1*) * * * * *

(*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.

* * * * *

Controller to act as repository.

20. (*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 intrusion 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.

Licence to issue Digital Signature Certificates.

21. (*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 (*1*), 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.

* * * * *

Suspension of licence.

23.(*1*)* * * * *

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

* * * * *

Access to computers and data.

29. (*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.

* * * * *

Certifying Authority to follow certain procedures.

30. Every Certifying Authority shall,—

* * * * *

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

* * * * *

Disclosure.

34. (*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;

* * * * *

(*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 reasonbale 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.

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

Certifying Authority to issue Digital Signature Certificate.

35. (*1*) * * * * *

(*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.

* * * * *

CHAPTER IX

PENALTIES AND ADJUDICATION

Penalty for damage to computer, computer system, etc.

43. 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;

* * * * *

Power to adjudicate.

46. (*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.

* * * * *

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

Establishment of Cyber Appellate Tribunal.

48. (*1*) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

* * * * *

Composition of Cyber Appellate Tribunal.

49. A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

50. 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.

Term of office.

51. The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

Salary, allowances and other terms and conditions of service of Presiding Officer.

52. 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.

Filling up of vacancies.

53. 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.

Resignation and removal.

54. (*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.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

55. No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

Staff of the Cyber Appellate Tribunal.

56. (*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, 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.

* * * * *

Recovery of penalty.

64. 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.

* * * * *

Hacking with computer system.

66. (*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 is 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 up to two lakh rupees, or with both.

Publishing of information which is obscene in electronic form.

67. Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh ruppes.

Power of Controller to give directions.

68. (*1*) * * * * *

(*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.

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

69. (*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.

Protected system.

70. (*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.

* * * * *

Penalty for mis-representation.

71. 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.

* * * * *

Penalty for publishing Digital Signature Certificate false in certain particulars.

73. (*1*) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

* * * * *

Publication for fraudulent purpose.

74. 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.

* * * * *

Penalties or confiscation not to interfere with other punishments.

77. 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.

2 of 1974.

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

Power to investigate offences.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. 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.

Network service providers not to be liable in certain cases.

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.

CHAPTER XIII

MISCELLANEOUS

2 of 1974.

80. (*1*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government 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.

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

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.

2 of 1974.

(*3*) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

* * * * *

82. 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.

Controller, Deputy Collector and Assistant Controllers to be public servants.

* * * * *

87. (*1*) * * * * *

Power of Central Government to make rules.

(*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, 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;

* * * * *

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

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

* * * * *

(*3*) Every notification made by the Central Government under clause (*f*) 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.

* * * * *

Power of State Government to make rules.

90. (*1*)* * * * *

(*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:—

* * * * *

(*c*) any other matter which is required to be provided by rules by the State Government.

* * * * *

Amendment of Act 45 of 1860.

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

Amendment of Act 1 of 1872.

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

Amendment of Act 18 of 1891.

93. The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

Amendment of Act 2 of 1934.

94. The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

———

THE FIRST SCHEDULE

(*See* section 91)

AMENDMENTS TO THE INDIAN PENAL CODE

(45 OF 1860)

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

Electronic record.

"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.". 21 of 2000.

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translate 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", the 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 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 or 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 death 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.'. 21 of 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.'. 21 of 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 words "document", in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the words "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", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'.

21 of 2000.

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

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

When oral admission as to contents of electronic records are relevant.

"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.

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

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

"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.".

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

Opinion as to digital signature when relevant.

"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.

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

Special provision as to evidence relating to electronic record.

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

Admissibility of electronic records.

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 form 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 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 form 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 sin 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 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 that information, of 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.'.

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

Proof as to digital signature.

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

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

Proof as to verification of digital signature.

'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.'.

21 of 2000.

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

Presumption as to Gazettes in electronic forms.

"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.".

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

Presumption as to electronic agreements.

"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.".

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

Presumption as to electronic messages.

'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 expression "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.'. 21 of 2000.

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

Presumption as to electronic records five years old.

"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.".

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

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

"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 data storage device;

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

'(*8*) "certified copy" means when the books of 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 a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'.

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

"2A. 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:— Conditions in the printout.

(*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 to ensure that data has been accurately transferred to such removable media;

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

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

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

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

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

———————

THE FOURTH SCHEDULE

(*See* section 94)

AMENDMENTS TO THE RESERVE BANK OF INDIA ACT, 1934

(2 OF 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-I, 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;".

* * * * *

LOK SABHA

A

BILL

further to amend the Information Technology Act, 2000.

(Shri Dayanidhi Maran, Minister of Communications and Information Technology)

MGIPMRND—4204LS(S5)—11-12-2006.