Report of the Expert Committee

Proposed Amendments to Information Technology Act 2000

August 2005

Department of Information Technology

Ministry of Communications & Information Technology

Government of India

New Delhi

PROPOSED AMENDMENTS

TO

INFORMATION TECHNOLOGY ACT, 2000

~~[Act No. 21 of 2000 dated 9th June, 2000]~~

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce" which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Whereas the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

And Whereas the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

And Whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

Be it enacted by Parliament in the Fifty-first Year of the Republic of India as follows: -

CHAPTER I : PRELIMINARY

1. Short title, extent, commencement and application:-

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

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

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to

[1-4]~~(a) a negotiable instruments as defined in section 13 of the Negotiable Instruments Act, 1881;~~

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

~~(c) a trust as defined in section 3 of the Indian Trusts Act, 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;~~

~~(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.

2. Definitions

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

(a) "**access**" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

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

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

[2(d)]~~(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~~

[1-4] sub-section 1(4) amended to bring flexibility in respect of applicability of IT Act on certain specific class of documents or transactions.

~~digital signature;~~

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

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

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and

in any other case, the Central Government;

(f) "**asymmetric crypto System**" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "**Certifying Authority**" means a person who has been granted a licence to issue an ~~Digital~~Electronic[1] 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~~ [2A]different types or forms of Electronic Signature Certificates;

(i) "**computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulation of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

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

(i) the use of satellite, microwave, terrestrial line, wireless[2B] or other communication media; and

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

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

---

[1] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[2A] The certificate practice statement as at present is associated with digital signature. However if the technology permits any other form of electronic signature the certification practice statement should also be there, though the contends of such CPS may be different

[2B] This has been done to include wireless communications explicitly

(l) "**computer system**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "**Controller**" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

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

(nn) **"[2C]Cyber Café"** means a place where access to electronic form is provided to the public

(o) "**data**" means a representation of information, knowledge, facts, concepts or instructions which ~~are~~ is being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

~~(p) "digital signature" means authentication of any electronic record by subscriber by means of an electronic method or procedure in accordance with provisions section 3;~~

[2D](p) "**digital signature**" means an electronic signature where authentication of electronic record is in the manner as provided in sub-section (2) of section 5.

~~(q) "Digital Signature Certificate" means a Digital Signature Certificate" issues under subsection (4) of section 35;~~

[2E](pa) "**digital signature certificate**" means an electronic signature certificate where authentication is by Digital Signature.

(q~~r~~) "**electronic form**" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer

[2C] The term "Cyber Café" has been included to address the issues relating to streamlining the functioning of cyber cafes.
[2D] Digital Signature is one of the types of Electronic Signature as defined in 2(t)
[2E] Digital Signature Certificate is one of the types of Electronic Signature Certificate as defined in 2(tt)

memory, micro film, computer generated micro fiche or similar device;

(rs) "**Electronic Gazette**" means the Official Gazette published in the electronic form;

(st) "**electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(t) [3]**"electronic signature"** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in any manner as the Central Government may prescribe as provided in section 5 and shall include Digital Signature.

(tt) "**electronic signature certificate**" means an Electronic Signature Certificate issued under section 35 and shall include Digital Signature Certificate.

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

(v) "**information**" includes data, message, 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~~ record [4A] means any person who on behalf of another person receives, stores or transmits that record ~~message~~ or provides any service with respect to that electronic ~~that~~ record ~~message~~;

(x) "**key pair**" in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "**law**" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder ;

(z) "**licence**" means a licence granted to a Certifying Authority under section

[3] The term electronic signature needs to be defined as including digital signature to make the Act technology neutral.

[4A] Term "intermediary" has been redefined.

24;

(za) "**originator**" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

[4B](zaa) "Person" means any individual, company or body corporate or association or body of Individuals, whether incorporated or not or artificial juridical person, whether domiciled or resident in India or outside India

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

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

(zd) "**public key**" means the key of a key pair used to verify a digital signature and listed in the ~~Digital~~ Electronic [4C]Signature Certificate authenticated by use of Digital Signature ;

(ze) "**secure system**" means computer hardware, software, and procedure that-

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

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

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

and

(d) adhere to generally accepted security procedures;

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

(zg) "**subscriber**" means a person in whose name the ~~Digital~~Electronic[5A] Signature Certificate is issued;

(zh) "**verify**" in relation to a ~~digital~~electronic[5A] signature, electronic record or public key, with its grammatical variations and cognate expressions means

---

[4B] A new subsection has been added to define term "Person"

[4C]. In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[5A]. In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

to determine whether-

(a) the initial electronic record was affixed with the digital digitalelectronic[5A] signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digitalelectronic[5A] signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II: APPLICATION OF LEGAL REQUIREMENTS TO ELECTRONIC RECORDs

~~CHAPTER II : DIGITAL SIGNATURE~~

3. Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

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

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

4. Legal recognition of ~~digital~~electronic[6A] signatures

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 digitalelectronic[6A] signature affixed in such manner as may be prescribed by the Central Government to ensure that the signature affixed is reliable.~~.~~

Explanation- 1. For the purposes of this section "signed", with the 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.

[6A] . In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

2. An Electronic Signature is considered reliable for the purposes of this Act if:[6B]

(a) the electronic data in relation to which the Electronic Signature is affixed is linked to the signatory and to no others;

(b) the Electronic Signature creation code given is unique to the signatory; and

(c) any alteration to the Electronic Signature or to the electronic data in relation to which the signature is affixed made after the time of signing is detectable;.

5. Authentication of electronic records by Electronic Signature

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his ~~digital~~ ~~signature~~electronic signature in the form of Digital Signature as provided in sub-section (2) or in such other electronic form as the Central Government may prescribe from time to time.

(2) (a) The authentication of the electronic record by Digital Signature shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

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

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

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

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

[6B] Explanation is added for defining reliability of Electronic Signatures. This has been done to allow only those technologies, which conforms to these conditions in lines with UNICITRAL Model Law of Electronic Commerce.

CHAPTER III : ELECTRONIC GOVERNANCE

6. Use of electronic records and ~~digital~~electronic[6C] signatures in Government and its agencies

(1) Where any law provides for-

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

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

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

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

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

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

(b) the manner or method of payment of any fee or charges for filing, creation or issue, or delivery of service either directly or through its authorized service provider[6D], of any electronic record under clause (a).

Explanation: For the purposes of this section

"authorized service provider" includes any person who has been permitted by the appropriate government through a license, registration certificate or a specific authorization letter to offer services through electronic means as per the policy governing the relevant service sector.

7. Retention of electronic records

[6C] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[6D] added to include delivery of service by authorized service providers

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-

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

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

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

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be ~~despatched~~dispatched[6E] or received.

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

8. Publication of rules, regulations, etc., in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette :

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Section 6, 7, and 8 not to confer right to insist document should be accepted in electronic form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law

[6E] word "despatched" has been replaced with "dispatched"

or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

~~**10. Power to make rules by Central Government in respect of digital electronic signature**[7A1]~~

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

~~(a) the type of digitalelectronic[7A] signature;~~

~~(b) the manner and format in which the digitalelectronic signature shall be affixed;~~

~~(c) the manner or procedure which facilitates identification of the person affixing the digitalelectronic signature;~~

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

~~(e) any other matter which is necessary to give legal effect to digitalelectronic signatures~~

[7AA]CHAPTER III A : ELECTRONIC CONTRACTS

~~10A~~. 10. Formation and Validity of Contracts

a. In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of an electronic record.

b. Where an electronic record is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose.

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

[7A1] Section 10 has been deleted as this is covered under section 87
[7AA] A new section 10A is added for "Formation and Validity of ElectronicContracts"

11. Attribution of electronic records

An electronic record shall be attributed to the originator-

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

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

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

12. Acknowledgement of receipt

(1) [7B]Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(2~~1~~) Where the originator has not stipulated that the acknowledgement 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.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee sating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of dispatch and receipt of electronic record
(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

[7B] Sub-section (1) and (2) have been rearranged for sequential reading and avoid confusion

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :-

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,-

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

(ii) if the electronic records is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be ~~despatched~~dispatched [8A]at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3)

(5) For the purposes of this section,-

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

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

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

CHAPTER V

[8A] word “despatched” changed with “dispatched”

SECURE ELECTRONIC RECORDS AND SECURE ~~DIGITAL~~ELECTRONIC[8B] SIGNATURES

14. Secure electronic records

Where any prescribed security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure ~~digital~~electronic[8B] signature

If, by application of a security procedure agreed to by the parties concerned or prescribed by the Central Government, it can be verified that a ~~digital~~electronic 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~~electronic signature would be invalidated.

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

16. Security procedure

~~The Central Government shall for the purpose 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~~

[8B] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

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

(1) For the purpose of secure electronic records or secure electronic signature, the Central Government may prescribe security procedures to be followed, keeping in view the commercial circumstances, nature of transactions and other related matters.

(2) The security procedures mentioned in sub-section (1) shall be prescribed after consultation with self-regulatory bodies of the industry, if any.

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller

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

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

(b) certifying public keys of the Certifying Authorities;

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

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

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

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an ~~Digital~~Electronic[8C] Signature Certificate and the public key;

(g) specifying the form and content of an ~~Digital~~Electronic[8C] Signature Certificate and the key;

(h) specifying the form and manner in which [8D]records relating to ~~issue of~~ electronic signature certificates ~~accounts~~ shall be maintained by the Certifying Authorities;

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

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

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

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

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

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

[8C] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[8D] There is a need to differentiate between accounts of the company and records relating to electronic signature certificate issued. The accounts of the company should continue to be governed by other laws such as Companies Act, Income Tax etc.

19. Recognition of foreign Certifying Authorities

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purpose of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the ~~Digital~~Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

~~**20. Controller to act as repository**~~[9A]

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

~~(2) The Controller shall-~~

[9A]

~~(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~~electronic ~~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.~~

21. Licence to issue ~~Digital~~Electronic[9B] Signature Certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue ~~Digital~~Electronic[9B]

[9A] Section 20 (Controller to Act as Repository) has been deleted. This has been done due to following reasons: (a) The responsibility of keeping the repository is the primary responsibility of Certifying Authority; (b) This is a redundant activity and put unnecessary legal obligation on Controller in case of any dispute between Certifying Authority and Subscriber; (c)Further, this practice is not being followed anywhere else.

[9B] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

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~~Electronic [9B]signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this sections shall-

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

(b) not be transferable or heritable;

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

22. Application for licence

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

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

(a) a certification practice statement ;

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

(c) payment of such fees, ~~not exceeding twenty-five thousand rupees~~[9C]as may be prescribed by the Central Government;

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

23. Renewal of licence

An application for renewal of a licence shall be-

(a) in such form;

(b) accompanied by such fees~~, not exceeding five thousand rupees,~~ [10A]as may be ~~specified~~ prescribed by the Central Government;

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

[9C] Fee amount omitted as it may change from time to time.
[10A] Fee amount omitted as it may change from time to time

licence.

24. Procedure for grant or rejection of licence

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

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Revocation and Suspension of licence

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

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

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

[10AA](c) failed to maintain the procedures and standards specified in ~~under clause (b) of sub-section (2) of section 20~~ section 30.

(d) contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence :

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

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

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any ~~Digital~~Electronic[10B] Signature Certificate during such suspension.

[10AA] Amended vide order no. S.O. 1015(E) dated September 19, 2002.

[10B] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

26. Notice of suspension or revocation of licence

~~(1)~~ Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

~~(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:~~

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site shall be accessible round the clock :

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

27. Power to delegate

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions[10BB]

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act under this Chapter, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitation laid down under that Act.

29. Access to computers and data

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that may 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

---

[10BB] Section 28 has been amended to define scope of Controller's power.

such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures

Every Certifying Authority shall,-

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

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

(c) adhere to security procedures to ensure that the secrecy and privacy of the ~~digital~~electronic[10C] signatures are assured;

(d) be the repository of all Electronic Signature Certificates issued by them under this Act.

(e) publish information regarding its practices, its certificates, and current status of such certificates; and

[10D]~~(d)~~ (f) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of licence

[10C] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[10D] CCA prescribe standards, rules, and regulations from time to time. All Certifying Authorities licenced by CCA must adhere to these standards.

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

33. Surrender of licence

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

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure

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

(a) its ~~Digital~~Electronic[10E] Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to ~~digital~~electronically[10E] sign another ~~Digital~~Electronic[10E]Signature Certificate;

(b) any certification practice statement relevant thereto;

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

(d) any other fact that materially and adversely affects either the reliability of an ~~Digital~~Electronic[10F] 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 an ~~Digital~~Electronic[10F] Signature Certificate was granted, then, the Certifying Authority shall-

---

[10E] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[10F] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

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

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

CHAPTER VII : ~~DIGITAL~~ELECTRONIC[10F] SIGNATURE CERTIFICATES

35. Certifying Authority to issue ~~Digital~~Electronic[10F] Signature Certificate

(1) Any person may make an application to the Certifying Authority for the issue of ~~a~~an ~~Digital~~Electronic[10F] Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee ~~not exceeding twenty-five thousand rupees~~ [10G]as may be prescribed by the Central Government, to be paid to the Certifying Authority :

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applications;

[10H]~~(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.~~

(4) On receipt of an application under sub-section (1), the Certifying Authority may,[10H] ~~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~~Electronic [10I]Signature Certificate or for reasons to be recorded in writing, reject the application in such a manner as prescribed by the Central Government:

~~Provided that no Digital Certificate shall be granted unless the Certifying Authority is satisfied that~~

[10G] Fee amount is omitted as it may change from time to time.

[10H] Requirement of CPS from subscriber deleted. As per Executive Order no. 2(8)/2000-Oers.I dated 12th September, 2002 from the Department of Information Technology, Government of India for the purpose of subsection (3) and (4) of Section 35 of the IT Act, 2000 every application for the issue of a Digital Signature Certificate shall not be required to be accompanied by Certificate Practice Statement (CPS) as required under existing sub-sections. The subsections are suitably amended.

[10I] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

~~(a) the application 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.~~

36. Representation upon issuance of an ~~Digital~~Electronic[10I] Signature Certificate

A Certifying Authority while issuing an ~~Digital~~Electronic [10I] Signature Certificate shall certify that-

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

(b) it has published the ~~Digital~~Electronic [10I] Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the case of Digital Signature Certificate; [10I]

(d) the subscriber's public key and private key constitute a functioning key pair in the case of Digital Signature Certificate; [10I]

(e) the information contained in the ~~Digital~~Electronic[11A] Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the ~~Digital~~Electronic[11A] Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of ~~Digital~~Electronic[11A] Signature Certificate

[11A] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a ~~Digital~~Electronic[11A] Signature Certificate may suspend such ~~Digital~~Electronic[11A] Signature Certificate,-

(a) on receipt of a request to that effect from-

(i) the subscriber listed in the ~~Digital~~Electronic[11A] Signature Certificate; or

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

(b) ~~if it is of opinion that the Digital~~Electronic[11A] ~~Signature Certificate should be suspended in public interest~~ on receipt of direction from the Controller.

(2) A ~~Digital~~ Electronic Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of ~~a~~an ~~Digital~~Electronic[11A] Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of ~~Digital~~Electronic[11A] Signature Certificate

(1) A Certifying Authority may revoke an ~~Digital~~Electronic[11A] Signature Certificate issued by it-

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

(b) upon the death of the subscriber; or

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

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a ~~Digital~~Electronic[12A] Signature Certificate which has been issued by it at any time, if it is of opinion that-

(a) a material fact represented in the Application for ~~Digital~~Electronic[12A] Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the ~~Digital~~Electronic[12A] Signature Certificate

[12A] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

was not satisfied;

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

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

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

(4) On revocation of ~~a~~an ~~Digital~~Electronic[12A] Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation

(1) Where a ~~Digital~~Electronic[12A] Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the ~~Digital~~Electronic[12A] Signature Certificate for publication of such notice.

(2) Where one or more **repositories** are specified, the Certifying Authority shall publish notice of such suspension or revocation, as the case may be, in all such repositories.

[12C]CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair in the case of Digital Signature Certificate

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, ~~then,~~ the subscriber shall generate that ~~the~~ [R1] key pair by applying the security procedure.

[12C] This chapter requires rearrangement because of technology neutral concept. The matter relating to digital certificate is placed first , then duties of the subscribers in case of certificate other than digital certificate

[R1] Amended vide order no. S.O. 1015(E) dated September 19, 2002

~~42~~ 41. Control of private key in the case of Digital Signature Certificate

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

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

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

41A. **Duties of the subscribers in the case of Electronic Signature:**

[12D][2]The subscriber shall be bound by such duties as the Central Government may prescribe in respect of electronic signature certificates and in the case of Digital Signature in addition to those provided in Sections 40 and 41.

4~~2~~1. Acceptance of ~~Digital~~Electronic[14A] Signature Certificate

(1) A subscriber shall be deemed to have accepted an ~~Digital~~Electronic[14A] Signature Certificate if he publishes or authorises the publication of an ~~Digital~~Electronic[14A] Signature Certificate-

(a) to one or more persons;

(b) in a repository, or

otherwise demonstrates his approval of the ~~Digital~~Electronic[14A] Signature Certificate in any manner,

[R2](2) By accepting an ~~Digital~~Electronic[14A] Signature the subscriber certifies to all who reasonably rely on the information contained in the ~~Digital~~Electronic[14A] Signature Certificate that-

---

[12D] As the other technology have not been developed fully as and when things mature the Government can prescribe duties

[14A] In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

[R2] Amended vide order no. S.O. 1015(E) dated September 19, 2002

(a) in the case of Digital Signature the subscriber controls ~~holds~~ the private key corresponding to the public key listed in the ~~Digital~~ Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the ~~Digital~~Electronic[14A] Signature Certificate are true.;

(c) all information in the ~~Digital~~Electronic[14A] Signature Certificate that is within the knowledge of the subscriber is true;.

(d) the electronic signature certificate is being used in accordance with the certification practice statement of the Certifying Authority for the time being in force;. and

(e) he acknowledges and accepts the terms contained in the Certification Practice Statement of the Certifying Authority.

~~42 Control of private key~~[42a]

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

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

~~Explanation- For the removal of doubts, it is hereby declared that the subscriber shall be liable to till he has informed the Certifying Authority that the private key has been compromised~~

CHAPTER IX : PENALTIES AND ADJUDICATION

43. ~~Penalty~~ Compensation for damage to computer, computer system etc. [14C]

[42a] This section has been deleted as it related to a CA and its subscriber

(1) If any person, without permission of the owner or of any other person who is incharge of a computer resource ~~computer, computer or computer network~~,-

(a) accesses or secures access to such computer resource; ~~computer, computer system or computer network~~;

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

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

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

(e) disrupts or causes disruption or impairment of any computer resource; ~~computer system or computer network~~;

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

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

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

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

[43-2](2) If any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore to the person so affected.

[14C] Section 43 Covers two issues relating to "Data Protection and Privacy" : (1) unauthorized access to a computer system, (2) unauthorized downloading/copying of data. The other sections that deals with the "Data Protection and Privacy" are Section 65, Section 66, and Section 72 of IT Act 2000.

[43-2] This section has been added to ensure reasonable security practices and procedures for sensitive information by any body corporate.

Explanation.- For the purposes of this section,-

(oi) “body corporate” means any company and includes a firm or other association of individuals engaged in commercial or professional activities.

(i) "computer contaminant" means any set of computer instructions that [3]are designed-

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

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

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed some other event takes place in that computer resource;
(iv) "damage " means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(v) “Reasonable security practices and procedures” means, in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

(vi) “Sensitive personal data or information” means such personal information, which is prescribed as “sensitive” by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

(vii) “Without the permission of the owner” shall include access to information that exceeds the level of authorized permission to access.

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

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

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

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate regarding compensation and penalty

[46-1](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 which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or

[46-1] words "under this Chapter" deleted to handle contraventions under section 72

judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and-

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

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

47. Factors to be taken into account by the adjudicating officer

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely :-

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

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

(c) the repetitive nature of the default.

CHAPTER X

THE CYBER ~~REGULATIONS~~ APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal

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

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be

appointed, by notification, by the Central Government.

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

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he-

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

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate 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.

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

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appointment 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.

54. Resignation and removal

(1)The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office :

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his officer sooner, continue to hold office until 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 terms of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his officer 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 misbehavior or incapacity of the aforesaid presiding Officer.

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

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

56. Staff of the Cyber Appellate Tribunal

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

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

(3) The salaries, 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.

57. Appeal to Cyber Appellate Tribunal

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

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

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed :

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

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

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

58. Procedure and powers of the Cyber Appellate Tribunal

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

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

(a) summoning and enforcing the attendance of any person and examining

him on oath;

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

(c) receiving evidence on affidavits;

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

(e) reviewing its decisions;

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

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purpose of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation

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

61. Civil court not to have jurisdiction

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court

Any person aggrieved by any decision or order of the Cyber Appellate

Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

[63]~~**63. Compounding of contraventions**~~

~~(1) Any contravention under this Chapter Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:~~

~~Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.~~

~~(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.~~

~~Explanation- For the purpose of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.~~

~~(3) Where any contravention has been compounded under sub-section (1); no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.~~

64. Recovery of penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the ~~Digital~~Electronic [16A]Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

[63] Section 63 has now been moved to Section 44 A

[16A]. In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

CHAPTER XI: OFFENCES

65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

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

~~**66. Hacking with computer system**~~

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

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

66 ~~Hacking with Computer System~~ Computer related offenses:

a) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource

   (i) accesses or secures access to such computer resource;

   (ii) downloads, copies or extracts any data, computer data base or information from such computer resource including information or data held or stored in any removable storage medium;

   (iii) denies or causes the denial of access to any person authorised to access any computer resource;

he shall be punishable with imprisonment upto one year or a fine which may extend up to two lacs or with both;

(b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is incharge of a computer resource

(i) introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;

(ii) disrupts or causes disruption or impairment of electronic resource;

(iii) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer resource;

(iv) provides any assistance to any person to facilitate access to a computer resource in contravention of the provisions of this Act, rules or regulations made thereunder;

(v) damages or causes to be damaged any computer resource, date, computer databse, or other programmes residing in such computer resource;

he shall be punishable with imprisonment upto two years or a fine which may extend up to five lacs or with both;

Explanation: For the purposes of this section-

a. 'Dishonestly' – Whoever does anything with the intention of causing wrongful gain to one person, wrongful loss or harm to another person, is said to do this thing dishonestly".

b. 'Fraudulently' – A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

c. "Without the permission of the owner" shall include access to information that exceeds the level of authorized permission to access.

67. Publishing in electronic form of information which is obscene ~~in electronic form~~[16AA]

(1) Save as provided in this Act under Section 79 which exempts intermediaries from liability in certain cases, 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,

[16AA] This option is formulated keeping in view the culture sensitiveness of our society.

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~~ two years and with fine which may extend to ~~one~~ five 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~~ five years and also with fine which may extend to ten lakh rupees.

(2) Whoever intentionally and knowingly publishes or transmits through electronic form any material which relates to child pornography, shall be punished with imprisonment for a term not less than three years and with a fine which may extend to ten lakh rupees and in the event of a 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.

Explanation: - For the purposes of this section "child pornography" means material that features a child engaged in sexually explicit conduct.

Exception – This sub-section (1) does not extent to –

(a) 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 bon fide for religious purposes;

68. Power of Controller to give directions

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who 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 three years or to a fine

not exceeding two lakh rupees or to both.

68A. Encryption and other technologies for security of data[19A]

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce by rules provide for one or more modes or methods for encryption.

~~**69.Directions of Controller to a subscriber to extend facilitates to decrypt information**~~ [19B]

~~(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~~

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource[19B]

(1) If the ~~Controller~~ Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity 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~~, 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 decrypt or cause to be monitored any information transmitted through any computer resource.

(2) The Central Government shall prescribe safeguards subject to which such interceptions or monitoring may be done.

[19A] Section 68A is added for providing one or more modes and methods for encryption.

[19B] Entire section is amended in respect of power to issue directions for interception or monitoring or decryption of any information through any computer resource.(Earlier this power was only with the Controller).

~~(2)~~ (3) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance

b. to decrypt the information; or

c. provide access to the computer resource containing such information

~~(3)~~ (4) The subscriber or any person who fails to assist the agency referred to in sub-section ~~(2)~~ (3) shall be punished with an imprisonment for a term which may extend to seven years.

[R5]**70. Protected system**

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

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

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation

(1) Whoever intentionally makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or ~~Digital~~Electronic[19C] 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.

72. ~~Penalty for~~ Breach of confidentiality and privacy

(1) Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other

[R5] Amended vide order no. 2(8)/2000-Pers.I dated September 12, 2002

[19C] . In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

material without the consent of the person concerned intentionally discloses such ~~electronic record, book, register, correspondence, information, document or other~~ material to any other person shall be punished with imprisonment for a term which may extend upto two years, or with fine which may extend to ~~one~~ five lakh rupees, or with both.

(2) Save as otherwise provided under this Act, if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected.;[72-2]

(3) Whoever intentionally captures or broadcasts an image of a private area of an individual without his consent, and knowingly does so under circumstances violating the privacy of that individual, shall be liable to pay compensation not exceeding Rs. 25 lakhs to the person so affected, and shall also be liable for imprisonment for a term not exceeding one year or with fine not exceeding Rs 2 Lakhs, or with both on the complaint of the person so affected.

(4) No court shall take cognizance of any offense punishable under sub-section (3) except upon a complaint filed by the aggrieved person in writing before a Magistrate

Explanation: For the purpose of this section

(a) "capture" with respect to an image, means to videotape, photograph, film, record by any means;
(b) "broadcast" means to electronically transmit a visual image with the intent that it be viewed by a person or persons;
(c) "a private area of the individual" means the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual;
(d) "female breast" means any portion of the female breast below the top of the areola; and
(e) "under circumstances violating the privacy of that individual" means –

(i) circumstances in which a reasonable person would believe that he or she could disrobe in privacy,

[72-2] Section 72(2) has been added to protect the privacy of the individual subscribers.

(ii) without being concerned that an image of a private area of the individual was being captured; or circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place.

(f) "Intermediary" as defined in Section 79;
(g) Injury as defined in IPC.

73. Penalty for publishing ~~Digital~~Electronic[21A] Signature Certificate false in certain particulars

(1) No person shall publish an ~~Digital~~Electronic [21A]Signature Certificate or otherwise make it available to any other person with the knowledge that-

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

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying an ~~digital~~electronic[21A] signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose
Whoever knowingly creates, publishes or otherwise makes available an ~~Digital~~Electronic[21A] 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 extend to one lakh rupees, or with both.

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

[21A] . In this clause and in number of other places the term " Digital" has been changed to "Electronic" to enable the Act to be technology neutral

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

76.Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78.-Power to investigate offences

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

CHAPTER XIA

EXAMINER OF ELECTRONIC EVIDENCE[21C]

78A. Central Government to notify Examiner of Electronic Evidence

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority notify any Department, Body or Agency of the Central or the State Government or any suitably qualified expert as an Examiner of Electronic Evidence. The

[21C] New section 78A as suggested by Dr. Vishwanathan Follow-up committee has been incorporated with minor changes.

procedures and conditions for the notification of such examiner shall be as prescribed by the Central Government.

Explanation: For the purposes of this section "Electronic 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 etc

CHAPTER XII

[21D]LIMITATION ON THE LIABILITY OF INTERMEDIARY ~~NETWORK SERVICE PROVIDERS NOT 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.~~

~~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;~~

79. Exemption from liability of intermediary in certain cases

1. An "Intermediary" shall not be liable under any law for the time being in force, for any third party information, data, or link made available by him, except when the intermediary has conspired or abetted in the commission of the unlawful act.

2. The provisions of sub-section (1) shall apply in circumstances including but not limited to where:

   a. Intermediary's function is limited to giving access to a communication network over which information made available by third parties is transmitted or temporarily stored; or The

[21D] This section is revised in lines with the EU Directives on E-Commerce 2000/31/EC issued on June 8th 2000

intermediary: (i) does not initiate the transmission, (ii) does not select the receiver of the transmission, and (iii) does not select or modify the information contained in the transmission.

3. The provisions of sub-section (1) shall not apply if, upon receiving actual knowledge of, or being notified by the Central Government or its agency that any information, data or link residing on a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails expeditiously to remove or disable access to that material on that resource.

Explanation: For the purpose of this section:-

a. Term 'Intermediary' has been defined in Chapter I, Section 2(w).

b. 'Intermediary' shall include, but not limited to, telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines including on-line auction sites, online-market places, and Cyber Cafes.

c. 'Third Party Information' means any information dealt with by an intermediary in his capacity as an intermediary.

CHAPTER XIII : MISCELLANEOUS

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

~~(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.~~

~~Explanation.- For the purpose of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.~~

~~(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the~~

~~person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.~~

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

80A. Compounding of Certain Offenses

(1) Notwithstanding any thing contained in the Code of Criminal Procedures, 1973, any offense punishable under this Act may either before or after the institution of any prosecution be compounded by

(a) the Controller; or
(b) the adjudicating officers appointed under section 46, where the maximum amount of fine and/or imprisonment does not exceed such limits as may be specified by the Central Government.

on payment or credit to the Central Government of such sum as the Controller or the Adjudicating officer, as the case may be, may specify.

(2) Nothing in sub-section (1) shall apply to an offence committed by a person within a period of three years from the date on which a similar offence committed by him was compounded under this section.

Explanation: For the purpose of this section

any second or subsequent offence committed after the expiry of a period of three years from the date on which the offence was previously compounded, shall be deemed to be a first offence.

(3) Where any offence is compounded before the institution of any prosecution, no prosecution shall be instituted in relation to such offence, either by the Controller or by the adjudication officer or by any other person, against the offender in relation to whom the offence is so compounded.

(4) Where the composition of any offence is made after the institution of any prosecution, such composition shall be brought by the Controller or the adjudicating officer in writing, to the notice to the Court in which the prosecution is pending and on such notice of the composition of the offence being given, the person in relation to whom the offence is so compounded shall be discharged.

81. ~~Act to have overriding effect~~ General Provisions

(1) The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

(2) Nothing that is permitted under the Copyright Act 1957 and the Patents Act 1970 as amended from time to time shall render any person liable for contravention of any of the provisions of this Act.

82. Controller Deputy Controller and Assistant Controller to be pubic servants

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

83. Power to give directions

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

85. Offences by companies

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment ~~if he proves~~ unless it is proved that the contravention took place with~~out~~ his knowledge and connivance and that he failed to prevent such contravention. ~~or that he exercised all due diligence to prevent such contravention.~~

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary

or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.- For the purposes of this section.-

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

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

86. Removal of difficulties
(1) If any difficulty arises in giving effect to provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty :

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

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

87. Power of Central Government to make rules
(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely :-

(ao) All specific class of documents or transactions as may be prescribed by the Central Government under sub-section 4 of section 1.

(a) the manner in which any information or matter may be authenticated by means of ~~digital~~ electronic 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 or method of payment of any fee or charges for filing, creation or issue, or delivery of service either directly or through its authorized service provider, of any electronic record under section 6.

(d) the matters relating to ~~the type of digital signature, manner and format in which it may be affixed under section 10~~ : (i) the type of electronic signature; (ii) the manner and format in which the electronic signature shall

be affixed; (iii) the manner and procedures which facilitate identification of the person affixing the electronic signature; (iv) control processes and procedures to ensure adequate integrity, security, and confidentiality of electronic records or payments; and (v) any other matter which necessary to give legal effect to ~~digital~~ electronic signatures under Section 10.

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

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

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

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

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

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

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

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

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

(n) the form in which application for issue of an ~~Digital~~ Electronic 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 an ~~Digital~~ Electronic Signature Certificate under sub-section (2) of section 35;

(oa) for grant of electronic signature certificate under sub-section (4) of section 35;

(ob) the duties of the subscribers under section 41A;

(oc) "Reasonable security practices and procedures" under section 43;

(od) "Sensitive personal information" under section 43;

(p) the manner in the adjudicating officer shall hold inquiry under sub-

section (1) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

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

(s) the procedure for investigation of misbehaviour or incapacity of the Presiding officer under sub-section (3) of section 54;

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

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

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

(va) modes or methods for encryption for secure use of electronic medium as provided in Section 68A.

(vb) prescribe safeguards subject to which such interception or monitoring can be done under sub-section (2) of Section 69;

(vc) notify protected system under Section 70;

(vcc) "Breach of Confidentiality and Privacy" under section 72;

(vd) notify the Examiner of Digital Evidence under Section 78A;

(ve) for "intermediary" under sub-section 2(w) and section 79; and

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

(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 if 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.

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

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

(3) The Cyber Regulations Advisory Committee shall advise-

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

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

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

[R4]**89. Power of Controller to make regulations**
(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

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

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

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

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

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

(e) the manner in which the Certifying Authority shall disclose the matters

[R4] Amended vide order no. S.O. 1015(E) dated September 19, 2002

specified in sub-section (1) of section 34;

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

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

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

90. Power of State Government to make rules

(1) [4]Subject to any rules made by the Central Government, the State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely :-

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

(b) for matters specified in sub-section (2) of section 6;

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

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two House, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860
The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

[4] The State Govt powers should be made subject to rules framed by the central Government

92. Amendment of Act 1 of 1872
The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

93. Amendment of Act 18 of 1891
The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1934
The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act

Term "Digital will be replaced by "Electronic" in Sections 91, 92,93, and 94.

		THE FIRST SCHEDULE **(See section 15)** **AMENDMENTS TO THE INDIAN PENAL CODE**	
Amendment to section 4		**1.**	In section 4, after clause (2) and before Explanation, the following clause shall be inserted, namely: -
			"(3) Any person in any place without and beyond India where the act or conduct constituting the offence involves targeting a computer resource located in India. *Explanation:* - the expression "computer resource" shall have the meaning assigned to it in clause (k) sub-section (1) of section 2 of the Information Technology Act, 2000,"
Amendment to section 40		**2.**	In section 40, in clause (2), after the figures "117", the figures "118, 119 and 120" shall be inserted.
Amendment to section 118		**3.**	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 encryption or any other information hiding tool, the existence of design", shall be substituted.
Amendment to section 119		**4.**	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 encryption or any other information hiding tool, the existence of design", shall be substituted.
Amendment to section 120		**5.**	In section 120, 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 encryption or any other information hiding tool, the existence of design", shall be substituted.
Insertion of a new section 417A		**6.**	After Section 417, the following section shall be inserted, namely:- **Punishment for cheating using digital signature of another person** **"417A** Whoever, cheats by using the digital 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 three years and shall also liable to fine."
Insertion of new section 419A		**7.**	After section 419, following section shall be inserted, namely: - **Punishment for cheating by impersonation using communication network or computer resource:** "**419A** Whoever, by means of any communication network 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 liable to fine. *Explanation:*- the expression "computer resource" shall have the meaning assigned to it in clause (m) of sub-section (1) of section 2 of the Information Technology Act, 2000,"
	17.	The Indian Evidence Act shall be amended in the manner specified in the second schedule.	
1 of 1872		**THE SECOND SCHEDULE** **(See section 16)** **AMENDMENT TO THE INDIAN EVIDENCE ACT 1872**	
Insertion of new section 45A		After section 45, the following section shall be inserted, namely: -	
		Opinion of Examiner of Digital Evidence	
		"**45A.** When the court has to form an opinion in a proceeding 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 the Digital Evidence referred to in section 78A of the Information Technology Act, 2000, is a relevant fact. ***Explanation.*** - An Examiner of Digital Evidence referred to in this section is an "expert."	

***