Information Technology Act, 2000.

The major part of business in today's world is carried on systems using computers as their backbone. In this day & age then cyber law & litigation assume an important role. Let us today look into the Information technology Act 2000, passed by our Parliament & which came into force on October 1, 2000. The Act is divided into 13 chapters, has 94 Sections & has 4 schedules.

This Act gives legal recognition to Electronic Documents (S.4) & Digital signature (Chp. 5). Now legally enforceable contracts can be entered via e-mail. These documents can be presented in a Court of Law (provided they have not been tampered with & are digitally encrypted). This being the case, Government Agencies can now start accepting documents in the electronic form and also accept electronic signatures on forms & other papers. Government Agencies will now keep a record of such documents & rules relating to the Act in the above matters will be published in the Official Gazette later on. But the Act makes it clear that no person can insist that his documents should be accepted in the electronic form only (S. 9). The Central Government has reserved the right to make rules regarding digital signatures & also to make amendments therein (S.10).

The Act in Chp. 5 lays down the basis for secure electronic records and secure digital signatures. The Central Government will lay down the procedure for issuing and attesting of such records and signatures (S.16). The Central Government has appointed a "Controller" under whom the Licenses for Certification Agencies for the purpose of digital signature will be allotted (S.17). S. 18 further specifies his functions; chief among which is the maintenance of database of certifying authorities. He can grant recognition to foreign certifying authorities under S.19. As per S.20 the Controller shall also keep a record of the "public key" (the part of the digital signature in public domain). The digital signature with the subscriber has 2 parts. The first part is the "private code" & the latter part is the "public key". A person can certify a document only by using a combination of the 2 parts. Any other person can view the document using the public key but any attempt to alter will result in it being rendered useless.

Sec. 21 to 34 deal with the provisions relating to licensing (S.21), application (S.22 & 23) & disclosure (S.34) of Certifying Authority. Chp. 7 discusses procedure for issue, usage, and abuse of a digital signature. The Certifying Authority can suspend / revoke a digital signature issued by it as given in Ss.37 & 38. As per S. 42 any attempt at accessing/ hacking/ destroying of the private key of the signature by any unauthorized person has to be notified to the "Certifying Agency" immediately by the subscriber. In such a scenario, the Certifying Agency will suspend the signature.

Chapter 9 (S.43) talks about the punishments & penalties to be charged in case of violation of the sections of the Act. It says that any person who accesses or secures access for an other person to a computer / computer network belonging to another; or downloads or copies data; introduces any contaminant; damages / disrupts the system or the software; denies access to the system to any authorized person; provides assistance to another to do any of the above (abatement) can be fined to pay damages not exceeding Rs. 1 Crore. Ss. 44 & 45 cover penalty and residuary penalty provisions.

One of the important Sections of the Act is S. 46. It states the appointment of "Adjudicating officer" for the purpose of settlement of disputes related to the Act & also arms him with powers possessed by a Civil Court. The Adjudicating officer will be the "first Court of Appeal" in relation to cases & disputes related to the Act. If he is satisfied that any person has broken the provisions of the Act, then he can punish & / or penalize the person according to the provisions contained in the Act. The appeal against the Adjudicating officer can be made to the Cyber Appeal Tribunal. The provisions relating to the Cyber Appellate Tribunal are covered in Chp. 10 (Ss.48 to 62). The tribunal will function on the basis of "Principles of Natural Law" as against those contained in the Civil Procedure Code, 1908. (S.58).

S. 61 makes it clear that "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." The judgements of the tribunal can be challenged only in the High Court (S.62).

If any person willingly changes the source code of a system, he may be fined to the extent of Rs. 2 lacs & or imprisoned for a period not exceeding 3 years (S. 65). Hacking is also an offence under the Act as per S. 66 & carries a sentence of imprisonment up to 3 years or fine up to Rs. 2 lacs or both. Publishing pornographic material on the Internet carries a sentence of 2 years imprisonment & or Rs.25000 fine for the first offence. The punishment is imprisonment up to 5 years & fine up to Rs. 50000 on repeating the offence (S.67). The Controller can open an electronic document if in his opinion the interests of the sovereignty & protection of the country or public interest are jeopardized. He can do this only by means of submitting a "written statement" to any Government Agency, which in turn will take necessary steps to access the document. If any person does not help him in this regard or obstructs him then that person may be charged to a prison sentence of up to 7 years (S. 69).

The Government can, under the act, declare it's certain computers or computer networks as "protected computers" (S. 70). Any person who commits any act (as mentioned u/s 43) against such computers / computer networks may be imprisoned for period up to 10 years. Any person who willfully gives wrong information to obtain a license as a "certification agent" or to obtain a digital signature fraudulently may be punished for a period up to 2 years & / or a fine of Rs. 1 lacs (S.71). Any person who obtains illegal access to any electronic document may be punished for a period up to 2 years & / or a fine of Rs. 1 lacs (S.72).

If in the opinion of the Controller or his authorized representative there has been a violation of the Act then he shall have access to such computers / apparatus as he may deem fit. The equipment could also be confiscated u/s 76. He can also take help of such people as required to investigate the matter (S. 29). The Controller or any officer authorized 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. Another important aspect of the Act is covered u/s 75. It makes it clear that the Act will be applicable even to foreigners or people in foreign locations if they willfully commit any breach of the Act e.g. as u/s 43. The Act also provides certain relief to the Internet/

electronic documentation Service Provider if he has merely acted as a means of information interchange, & in such a case he will not be held liable (S.79).

Another important point under the Act is that only an officer of the rank of Deputy Superintendent of Police (or above) shall investigate any offence under the Act. (S.78). He 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 the Act (S. 80). He must be presented before the magistrate as soon as possible & the rules of the Criminal Procedure Code do not apply here. The Act also mentions the setting up of the "Cyber Regulation Advisory Committee" under Section 88 which will advise the Government from time to time as to the changes required to be made due to changes in technology & development of new inventions & apparatus.

The Act also provides that anything contained in any other Act that is in contradiction to or which renders the application of the I.T. Act will be considered ineffective (S.81). The amendments made in the Indian Penal Code; Indian Evidence Act; Bankers Book Evidence Act & the Reserve Bank of India Act (Ss. 91 to 94) are contained in the 4 schedules. The Act makes it clear that as of now the Act will not apply on

(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 sate of 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.

The Act also has it share of glitches & shortcomings. Chief among them are: the provision relating to powers of the D.S.P. to search & seizure on the basis of "reasonable doubt" that an offence has been / will be committed against this Act. The width of the powers given

leaves it open for misuse & corruption. The sections not only allow for search but also provide the powers of "arrest" on the basis of suspicion. Such wide powers regarding cyber crime have not been given to officers of any other country in the world where Cyber Law is in place. (India & 11 other countries have Cyber law in place.)

The Act also places additional responsibility upon the Service Providers & they have been made liable for almost all content / information on their servers. The construction of S. 79 leaves much scope for harassment. The Act also has several shortcomings with reference to the entire gamut of law relating to "Intellectual Property". (The branch related to patents, trademarks & copyrights). The Act also does not make any mention of payment mechanism for Indian companies who will have to pay foreign companies for services/ products rendered. Another important shortcoming is the total absence of any provisions relating to "domain names" which is a very important area of Cyber litigation as it amounts to trademark / copyright infringement.
The application of the Act will also have its share of problems as the Act applies not only to Indian citizens but even to foreigners who contravene the provisions of the Act with reference to India (S.75).

The Act also makes only a limited number of offences as cognizable but the field of Cyber Law is facing newer crimes & methods every day. This issue has not been properly addressed. All said and done, the Act will have far reaching implications & is an important piece of legislation which is very essential especially now as we put a sharp emphasis on software industry for our economic growth. Thus we have seen a short summary of the Information Technology Act, 2000; a new subject of legislation which will have a profound impact on cyber law & electronic business in our country.