CYBER LAWS AND ELECTRONIC EVIDENCE

- **INTRODUCTION**

The Term 'Cyber Crime' needs no introduction in today's E-world. In this world, where everything is available at a click, crimes are also been committed at a click. Cyber Crime thus is the darker side of technology. It is a Crime where the computer is either a tool or a target. The term WWW which stands for World Wide Web has now become World Wide Worry because of mushroom growth in cyber crimes. Crime in a developing nation is a hindrance to its development. It not only adversely affects all the members of the society but it also pulls down the economic growth of the country. Computer Technology provided a boost to the human life. It made the life of human being easier and comfortable. It not only added speed to the life of human being, but it also added accuracy and efficiency. But this computer was exploited by the criminals. This illegal use of computers for commission of crime leads to Cyber Crime. To combat Cyber Crime India got armed herself with The Information Technology Act 2000. This act got drastically amended in year 2008. The Amended Information Technology Act is not only effective than the previous Act it is more powerful and stringent than the previous one.

- **HISTORY OF CYBER LAWS IN INDIA**

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.

With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000.

This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

- **STATUTORY FRAMEWORK : INFORMATION TECHNOLOGY ACT 2000**

➢ **Structure of Act**

The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the Information Technology Act , 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from thereon the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per Information Technology Act -2000 and since replaced by electronic signatures in the Information Technology Act Amendment -2008) have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011.

➢ **Object of the Act**

The object of The Information Technology Act, 2000 as defined therein is as under :-

"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 methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

➢ **Applicability**

The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (i.e. where it is not applicable) as detailed in the First Schedule, stated below:

• Negotiable instrument (other than a cheque) as defined in Section 13 of the Negotiable Instruments Act, 1881;

• Power-of-attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;

• Trust as defined in Section 3 of the Indian Trusts Act, 1882

• Will as defined in clause (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition

• Any contract for the sale or conveyance of immovable property or any interest in such property;

• Any such class of documents or transactions as may be notified by the Central Government.

- **Highlights of the Act**

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by the use of a public key of the subscriber.

Chapter III of the Act details about the electronic governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in 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

The said chapter also details the legal recognition of digital signatures.

Chapter IV of the said Act gives a scheme for the regulation of certifying authorities. The Act envisages a Controller who shall supervise the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities. The Controller will also specify the various forms and content of digital signature certificates. The Act accepts the need for recognizing foreign certifying authorities and it further details the various provisions for the issuance of license to issue digital signature certificates.

Chapter VII of the Act details the scheme of things relating to digital signature certificates. The duties of subscribers are also enshrined in the Act.

Chapter IX talks about penalties and adjudication for various offences. The penalties for damage to a computer system have been fixed as damages by way of compensation not exceeding Rs 1,00,00,000. The Act talks of appointment of an officer not below the rank of a Director to the Government of India or an equivalent officer of a state government as an Adjudicating Officer to judge whether any person has made a contravention of any of the provisions of the Act. The officer has been given the powers of a civil court.

The Act in **Chapter X** talks of the establishment of Cyber Regulations Appellate Tribunal, an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred.

Chapter XI of the Act talks about various offences, which could be investigated only by a police officer not below the rank of Deputy Superintendent of Police. These offences include tampering

with computer source documents, publishing of information that is obscene in electronic form and hacking.

Hacking has been properly defined in Section 66 as, "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." Further for the first time, punishment for hacking as a cyber crime prescribed in the form of imprisonment upto 3 years or with fine which may extend to Rs. 2,00,000/- or with both. This is a welcome measure as hacking has assumed tremendous importance in the present day scenario. On previous occasions, the web sites of the Government have been hacked into but no legal provision within the existing legislation could be invoked to cover "hacking" as a cyber crime. It shall now be possible to try and punish hackers under section 66 of the Information Technology Act , 2000.

The said Act also provides for the constitution of the Cyber Regulations Advisory Committee which shall advice the government as regards any rules or for any other purpose connected with the said act. The said Act also has four Schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the Information Technology Act , 2000.

- **TYPES OF CYBER CRIME**

Cybercrimes can be basically divided into four major categories:

1. **Cyber Crimes against persons.**

   Cyber crimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cyber crimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen. There are certain offences which affect the personality of individuals can be defined as:

   Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

   Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual. **Carding**: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. **Cyber Crimes against property.**

The second category of Cyber-crimes is that of Cyber crimes against all forms of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy software. There are certain offences which affects persons property which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

Cyber Vandalism: Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They mainly affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computer system of the individuals.

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. **Cyber Crimes against government**

The third category of Cyber-crimes relates to Cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament attack in Delhi and the recent Mumbai attack fall under this category.

4. **Cyber Crimes Against Society at large:**

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

Child Pornography: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

Cyber Trafficking: It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime.

Online Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name

of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Financial Crimes: This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

- **PARALLEL PROVISIONS IN THE IPC AND IT ACT**

Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both.

It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "*whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment of either description*[1] *for a term which may extend to 2 (two) years, or with fine, or with both.*" This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that "*whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*". Needless to say, damaging computer systems and even denying access to

a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

Identity theft and cheating by personation: Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Forgery has been defined in section 463 of the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any

property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment mat extend to 7 (seven) years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

Obscenity: Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 (three) months, or with fine, or with both.

- **Cyber crimes not provided for in the IPC**

The following cyber-crimes penalised by the IT Act do not have an equivalent in the IPC.

Section 43(h) of the IT Act: Section 43(h) read with section 66 of the IT Act penalises an individual who charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. A person who tampers with the computer system of an electricity supplier and causes his neighbour to pay for his electricity consumption would fall under the aforesaid section 43(h) of the IT Act for which there is no equivalent provision in the IPC.

Section 65 of the IT Act: Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.

To a certain extent, section 409 of the IPC overlaps with section 65 of the IT Act. Section 409 of the IPC provides that any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine. However, section 65 of the IT Act does not require that the person who tampers with or damages or destroys computer source documents should have been entrusted with such source code. Under section 409 of the IPC, criminal breach of trust should have been committed by someone to whom the property was entrusted.

Violation of privacy: Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.

There is no provision in the IPC that mirrors Section 66E of the IT Act, though sections 292 and 509 of the IPC do cover this offence partially.

Section 292 of the IPC has been discussed above. Section 509 of the IPC provides that if any person intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, such person shall be punished with simple imprisonment for a term which may extend to 1

(one) year, or with fine, or with both. Unlike section 66E of the IT Act which applies to victims of both genders, section 509 of the IPC applies only if the victim is a woman.

Section 67C of the IT Act: Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. The section further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonment for a term which may extend to 3 (three) years and also be liable to a fine. An 'intermediary' with respect to any particular electronic record, has been defined in the IT Act to mean any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes. There is no corresponding provision in the IPC.

Cyber terrorism: Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'. Whoever knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, is also guilty of 'cyber terrorism'.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

There is no provision in the IPC that mirrors section 66F of the IT Act, though section 121 of the IPC (waging, or attempting to wage war, or abetting waging of war, against the Government of India) does cover this offence partially.

- **NATURE OF OFFENCE-WHETHER COMPOUNDABLE, COGNIZABLE AND BAILABLE**

Section 77A of the IT Act provides that, subject to certain exceptions, all offences under the IT Act for which the punishment is imprisonment for a term of 3 (three) years or less, are compoundable. The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 ("CrPC") shall apply with respect to such compounding.

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offences punishable with imprisonment of 3 (three) years or less shall be bailable.

Most of the cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less. The cyber-crimes which are punishable with imprisonment of more than 3 (three) years are:

a. Publishing or transmitting obscene material in electronic form under section 67 of the IT Act;
b. Publishing or transmitting of material containing sexually explicit act, etc., in electronic form under section 67A of the IT Act;
c. Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form under section 67B of the IT Act; and
d. Cyber terrorism under section 66F of the IT Act.

All of the cyber-crimes under the IPC are bailable other than offences under section 420 (*cheating and dishonestly inducing delivery of property*), section 468 (*forgery for the purpose of cheating*), section 411 (*dishonestly receiving stolen property*), section 378 (*theft*) and section 409 (*criminal breach of trust by public servant, or by banker, merchant or agent*), which are non-bailable.

Offences under sections 463 and 465 (*forgery*), sections 425 and 426 (*mischief*), section 468 (*forgery for the purpose of cheating*), section 469 (*forgery for the purpose of harming reputation*) and section 292 (*sale, etc., of obscene books, etc.*) of the IPC are non-compoundable offences while offences under sections 378 and 379 (*theft*), 420 (*cheating and dishonestly inducing delivery of property*), sections 425 and 426 (*mischief when the only loss or damage caused is loss or damage to a private person*), section 509 (*word, gesture or act intended to insult the modesty of a woman*), section 411 (*Dishonestly receiving stolen property*) and section 419 (*Punishment for cheating by personation*) of the IPC are compoundable offences. Of these, offences under sections 420 and 509 can be compounded only with the permission of the court. Most of the cyber crimes under the IPC are cognizable other than the offences under sections 425 and 426 (*mischief*) and sections 463 and 465 (*forgery*) which are non-cognizable.

The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bailable under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa. For instance, in case of hacking and data theft, offences under

sections 43 and 66 of the IT Act that are bailable and compoundable while offences under section 378 of the IPC are non-bailable and offences under section 425 of the IPC are non-compoundable. Further, in case of the offence of receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under section 411 of the IPC is non-bailable. Similarly, in case of the offence of identity theft and cheating by personation, the offences under sections 66C and 66D of the IT Act are compoundable and bailable while the offences under sections 463, 465 and 468 of the IPC are non-compoundable and the offences under sections 468 and 420 of the IPC are non-bailable. Finally, in case of obscenity, the offences under sections 67, 67A and 67B of the IT Act are non-bailable while the offences under section 292 and 294 of the IPC are bailable. This issue has been dealt with by the Bombay High Court in the case of *Gagan Harsh Sharma v. The State of Maharashtra*[2] (discussed below) wherein offences under sections 408 and 420 of the IPC that are non-bailable and cannot be compounded other than with the permission of the court were in conflict with offences under sections 43, 65 and 66 of the IT Act that are bailable and compoundable.

- **ROLE OF JUDICIARY IN EXPANDING CYBER CRIME JURISPRUDENCE**

A. Google India Pvt Ltd. Vs.Vishaka Industries and Anr. AIR 2020 SC 350

The Apex Court of India herein rejected the plea of immunity against liability as internet intermediary by Google India. Prior to the amendment to Section 79 of the Information Technology Act made in 2009, the protection to a network service provider was only for liability under the IT Act, this protection did not extend to liabilities arising under other enactments.

Asbestos sheets are produced by Vishakha Industries, and there were articles published by an individual "Ban Asbestos' in group which was hosted in the Google Groups services provided by Google. Since the group was hosted by Google India, it was also made a party to the suit. It was alleged that Google India has failed to take down the articles which were hosted by the Google, even after several notices were served.

Google appealed under Section 482 of the Code of Criminal Procedure to the Andhra Pradesh High Court seeking to quash the complaint claiming that no liability over the defamatory article being an intermediary under Section 79 of the Information Technology Act should be incurred by Google. This was claimed on the basis that it was neither an author nor the publisher of the blog, in order to incur the liability.

The request to quash the proceeding was rejected by the High Court, explaining that Google as an intermediary had failed to act on the notice provided against an objectionable post when notified by the aggrieved person, hence under the IT Act Google India shall incur liability as it did not "move its little finger" even after several notices sent by the complainant. Due to the omission of acts by Google it could not claim any exemption under the IT Act.

The Supreme Court held that the matter is deemed to be decided on the basis of Section 79 of the IT Act, prior to the amendment of 2009 as the complaint was filed before the

amendment. After the amendment, the scope of protected for intermediaries has increased, as it states that the intermediaries shall be granted exemption from liability 'notwithstanding anything contained in any law for the time being in force'. The only exception to seek protection is if the intermediary had "knowledge" of the objectionable material. "Actual Knowledge" was dealt in the case of Shreya Singhal, to mean an order from court or a competent authority under law. But the precedent of Shreya Singhal Case can not be applicable as the complaint arose before the amendment.

The second contention that was raised before the Supreme Court of India was that Google was not intermediary but only a subsidiary of Google LLC. The court opted to not adjudicate this contention and said it was a matter for trial. The Supreme Court also set aside the finding made by the High Court that Google had failed to act despite receiving notice.

The Supreme Court mentioned that under Section 499 of the Indian Penal Code, which states the liability arising for criminal defamation, no immunity could be claimed in complaints which arose before the 2009 amendment in the court of law. The Bench comprising of Justice Ashok Bhushan and Justice K M Joseph stated, "We hold that Section 79 of the Act, prior to its substitution, did not protect an intermediary in regard to the offence under Section 499/500 of the IPC".

B. Sharat Babu Digumarti v. Govt. of NCT of Delhi AIR 2017 SC 150

While determining the question whether the appellant who has been discharged under Section 67 of the IT Act could be proceeded under Section 292 IPC, the Bench of Dipak Misra and Praffula C. Pant, JJ. held that when the Information Technology Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 IPC. It is to be noted that electronic forms of transmission is covered by the IT Act, a special law and that a special law shall prevail over the general and prior laws.

The case dealt with an appeal against the High Court's order charging the appellant under Section 292 IPC, despite the charges being dropped under Section 67 of the IT Act. The appellant, senior manager of the intermediary, had been singularly framed under Section 292 IPC while the managing director of the intermediary has been discharged of all the offences as per the decision in *Aneeta Hada* v. *Godfather Travels and Tours (P) Ltd*., (2008) 13 SCC 703. Counsel for the appellant urged that Section 79, as the language suggested, keeping in view the paradigm of internet world where service providers of platforms do not control and indeed cannot control the acts/omissions of primary, secondary and tertiary users of such internet platforms, protected the intermediary till he had the actual knowledge. Whereas counsel for the respondent pleaded that the role of person in charge of the intermediary was extremely vital as it pertained to sale of obscene material which was punishable under Section 292 IPC and not under Section 67 of the IT Act.

The Court said that the offence in question related to electronic record and Section 67 clearly stipulated punishment for publishing, transmitting obscene materials in electronic form. The said provision read with Sections 67-A and 67-B was a complete code, Section

79 being an exception provision conferred protection to the individuals. Section 292 IPC makes offence the sale of obscene books, etc. but once the offence has a nexus with the electronic record the protection under Section 79 cannot be ignored and negated. The Court quashed the criminal prosecution lodged against the appellant.

C. W.B. State Election Commission v. Communist Party of India (Marxist), 2018 SCC OnLine SC 1137AIR2018 SC 3964

The Bench comprising of CJ Dipak Misra and AM Khanwilkar and Dr DY Chandrachud, JJ., addressing the challenge to the Calcutta High Court's decision on issuing directions for the acceptance of nominations in the electronic form by the West Bengal State Election Commission, decided to set aside the impugned judgment and order of the High Court.

The present appeal consisted of the facts that the candidate who wished to contest the panchayat elections were not being allowed to collect and submit their nomination forms as a result of the violent actions of the supporters of the ruling party in the State. The relief that the respondents were pressing upon was that the State Election Commission must accept nominations already filed, in the electronic form.

The Supreme Court on observing the facts and contentions of the parties and on analyzing the whole scenario of circumstances in the present matter stated that the provision contained in the Panchayat Elections Act 1973 and Rules constitute a complete code in regard to the conduct of the election, including the matter of filing nominations. Neither the Panchayat Elections Act nor the Rules contemplate the filing of nominations in the electronic form and for any such reform, a legislative amendment has to be carried out.

Further, in the matter concerning the uncontested seats in the said elections, the Bench stated that the intervention of this Court is sought on the basis that free and fair elections are a part of the basic feature of the Constitution. While the Court was of the view that the validity of the elections must be tested in election petitions under Section 79(1) of the Act, however, the seriousness of the allegations and proceedings placed before the Court would necessitate exercising the power under Article 142 of the Constitution of India. Accordingly, the Court extended a period of 30 days for filing nominations in regard to the uncontested seats. For the reasons mentioned hereinabove, the judgment and order of the Calcutta High Court impugned in the appeal was set aside. The appeal was disposed of in the terms above.

D. Ramesh Rajagopal vs. Devi Polymers Private Limited AIR 2016SC 1920

While dealing with the appeal filed against orders of High Court whereby it dismissed appellant's Petition to quash criminal proceedings, the Hon'ble Apex Court observed as follows:

As regards the commission of offences under the Information Technology Act, 2000 the allegations are that the Appellant had, with fraudulent and dishonest intention on the website of Devi Consultancy Services i.e. www.devidcs.com that the former is a sister concern of Devi Polymers. Further, that this amounts to creating false electronic record.

In view of the finding above we find that no offence is made out Under Section 66 of the I.T. Act, read with Section 43. The Appellant was a Director of Devi Polymers and nothing is brought on record to show that he did not have any authority to access the computer system or the computer network of the company. That apart there is nothing on record to show the commission of offence Under Section 65 of the I.T. Act, since the allegation is not that any computer source code has been concealed, destroyed or altered. We have already observed that the acts of the Appellant did not have any dishonest intention while considering the allegations in respect of the other offences. In the circumstances, no case is made out Under Sections 65 and 66 of the I.T. Act, 2000.

E. B.N. Firos vs. State of Kerala and Ors. 2018(9)SCC 220

The Appellant-B.N. Firos-proprietor of Comtech IT Solutions, Thiruvananthapuram had filed a Writ Petition challenging a Notification dated 27th December, 2002 issued Under Section 70(1) of the Information Technology Act, 2000 (hereinafter referred to as "I.T. Act") declaring the computer, computer system and computer network specified in the Schedule to the Notification to be "protected systems" under the I.T. Act. The vires of Section 70 of the I.T. Act itself was also challenged. The Writ Petition was dismissed. The said order of dismissal has been affirmed in writ appeal by a Division Bench of the High Court and the review filed there against has also been dismissed. Aggrieved, this appeal(s) has been filed.

The Court herein observed that the amendment to Section 70(1) of the I.T. Act brought in by Act No. 10 of 2009, in our considered view, makes the power of declaration of protected system even more stringent by further circumscribing the power of declaration of protected system only in respect of a computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, which is a defined expression in the I.T. Act (already extracted). The amendment, in our considered view is not a first time introduction of parameters to govern the exercise of power Under Section 70(1) of the I.T. Act. Rather, it is an attempt to circumscribe the power even further than what was prevailing under the pre-amended law, by narrowing down the ambit of "government work" so far as it is relatable to the facility of Critical Information Infrastructure, as defined under the Act.

F. Union of India (UOI) and Ors. vs. G.S. Chatha Rice Mills and Ors.MANU/SC/0714/2020

The provisions in the Customs Act for the electronic presentation of the bill of entry for home consumption and for self-assessment have to be read in the context of Section 13 of the Information Technology Act which recognizes "the dispatch of an electronic record" and "the time of receipt of an electronic record". The legal regime envisaging the electronic presentation of records, such as the presentation of a bill of entry, has been imparted precision as a result of the enabling framework of the Information Technology Act under which these records are maintained. The presentation of the bill of entry Under Section 46 is made electronically and is captured with time stamps in terms of the requirements of the Information Technology Act read with Rule 5(1) of the Information Technology (Electronic Service Delivery) Rules 2011.

G. The State of Uttar Pradesh vs. Aman Mittal and Ors. 2019(19)SCC740

The question examined was as to whether an activity emanating from electronic form which may be obscene would be punishable Under Section 292 Indian Penal Code or Section 67 of the IT Act or both or any other provision of the IT Act. This Court held that Section 292 Indian Penal Code makes offence sale of obscene books, etc. but once the offence has a nexus or connection with the electronic record the protection and effect of Section 79 cannot be ignored and negated in view of special provision for a specific purpose. The IT Act has to be given effect to so as to make the protection effective and true to the legislative intent

H. The Bank NSP Case: State by Cyber Crime Police vs. Abubakar Siddique

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

I. Bazee.com case: Avnish Bajaj vs. State (N.C.T.) Of Delhi 3 Comp LJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.

J. Parliament Attack Case: State vs. Mohammad Afjal Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

K. Andhra Pradesh Tax Case: Andhra Pradesh State Road vs. The Income-Tax Officer 1964 AIR SCR (7) 17.

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were

conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

L. State of Tamil Nadu v. Suhas Katti

The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group, after she turned down his proposal for a marriage. The accused opened a fake email account in the name of the woman, and forwarded emails received in that account. The victim also received phone calls by people who believed that she was soliciting for sex work .The police complaint was lodged in February 2004 and within a short span of seven months from the filing of the First Information Report, the Chennai Cyber Crime Cell achieved a conviction. Katti was punished with two years' rigorous imprisonment and Rs. 500 fine under S. 469 IPC (forgery for the purpose of harming reputation), one year's simple imprisonment and Rs. 500 for offence under S. 509 IPC (words, gestures or acts intended to insult the modesty of a woman) and two years' rigorous imprisonment and Rs. 4000 fine for offence under S. 67 of IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).

M. Fatima Riswana v. State Represented by ACP, Chennai and other,

Both the public prosecutor and counsel for the petitioners applied to the court for transfer to another (male) judge, to save the district lady judge from embarrassment of having to view certain CDs that are part of the evidence. The order for transfer was passed and the justification for this was that the "said trial would be about the exploitation of women and their use in sexual escapades by the accused, and the evidence in the case is in the form of CDs. and viewing of which would be necessary in the course of the trial, therefore, for a woman Presiding Officer it would cause embarrassment."

N. S.M.C. Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

India's first case of cyber defamation case, In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff. On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature.

O. Air force Bal Bharti School Case

This was filed in the Juvenile court, Delhi on the charge of cyber pornography. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court. The brief facts in issue were that a student of the Air force Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in the year 2001 April. The alleged accused was then a class XII student who created a pornographic website as

revenge of being teased by classmates and teachers. He listed in that website the name of his 12 school mates 'girls and teachers in sexually explicit manner. He was then suspended by the School Authorities though the juvenile court allowed his bail prayer. However, he was charged under s. 67 of the Information Technology Act 2000, and ss. 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women Act. The most significant steps were taken by the law enforcement agencies in India. Further, Honble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiff.

P. Shreya Singhal v. U.O.I AIR 2015 SC 1523

This is a landmark judgment, concerning section 66A of the Information Technology Act, 2000. This Section was not in the Act as originally enacted, but came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009. Section 66A of the Information Technology Act, 2000 was struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

- **ELECTRONIC EVIDENCE**

➢ **Introduction**

The 21st century saw a technological revolution which enthralled not only India but the whole world. The use of computers is not limited to established organizations or institutions but available to every individual at swipe of a finger. Information Technology has eased out almost every humanized action. In this age of cyber world as the application of computers became more popular, there was expansion in the growth of technology. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. This increasing reliance on electronic means of communications, e-commerce and storage of information in digital form has most certainly caused a need to transform the law relating to information technology and rules of admissibility of electronic evidence both in civil and criminal matters in India. The proliferation of computers and the influence of information technology on society as whole, coupled with the ability to store and amass information in digital form have all necessitated amendments in Indian law to incorporate the provisions on the appreciation of digital evidence. The Information Technology Act, 2000 and its amendment are based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce. The Information Technology (IT) Act 2000 was amended to allow for the admissibility of digital evidence. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.

➢ **Statutory Provision- The Indian Evidence Act, 1872**

Section 3 The definition of evidence as given in the Indian Evidence Act, 1872 covers a) the evidence of witness i.e. oral evidence, and b) documentary evidence which includes electronic

record produced for the inspection of the court. Section 3 of the Act was amended and the phrase "All documents produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court". Regarding the documentary evidence, in **Section 59**, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

S.17 Admission Defined. The definition of 'admission' (Section 17 of the Evidence Act) has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance.

S.22A. When oral admissions as to contents of electronic records are relevant.— New Section 22-A has been inserted into Evidence Act, to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question. So remember until your evidence‟s admissibility is in question, none of the corroboration that you provide about its genuineness along is going to be valid.

S. 34. Entries in books of accounts including those maintained in an electronic form, regularly kept in the course of business, are relevant.

S. 35 An entry in any public or other official book, register or record or an electronic record made by a public servant in the discharge of his official duty, or by any other person in performance of a duty is kept, is itself a relevant fact.

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

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

S. 45A. Opinion of Examiner of Electronic Evidence.

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

S. 47A. Opinion as to electronic signature where relevant

When the Court has to form an opinion as to the [Electronic signature] of any person, the opinion of the Certifying Authority which has issued the [Electronic Signature Certificate] is a relevant fact.

S. 67A. Proof as to digital signature

Expert in the case of a secure 2[electronic signature], if the [electronic signature] of any subscriber is alleged to have been affixed to an electronic record the fact that such [electronic signature] is the 2[electronic signature] of the subscriber must by proved.

Section 65B of Indian Evidence Act is under focus in the Judicial and Law Enforcement circles.The main points that makes here are:

a) Section 65B (as well as 65A) of Indian Evidence Act refer to the special provisions of the Act in respect of Electronic Documents. Though Section 65 is referring to "Secondary" documents in paper form, there is no such distinction made as to the electronic document.

b) There is no need to distinguish Primary and Secondary and all documents need to be interpreted by a human being which takes the form of a Section 65B certificate.

c) A "Hard disk" which may contain an electronic document also cannot be considered the "Primary Document" since it is only a "Container" and the real Electronic document is an expression in binary language which cannot be read by a human being and needs to be interpreted with the assistance of a binary reading device (Computer + operating system +Application).

d) Section 65B explains the conditions under which an electronic document can be considered as "Admissible" in a Court as a "Document" and it needs to be suitably confirmed for the Court to accept the document, which is often termed as "Section 65B certificate or Statement"

e) Section 65B refers to a process of producing a "Computer Output" of the electronic document which is the evidence to be admitted and such computer output can be either in the form of a "Print Out" or a "Copy".

f) There is a "Process" by which the electronic document becomes the "Computer output" and Section 65B identifies this as the subject activity which needs to be conducted by a person having lawful control over the computer producing such output and that during the period of such production, the Computer should be working properly etc.

g) The focus of Section 65B is the activity of conversion of the electronic document residing inside a system which can be seen by an observer into a "Computer Output".

h) The other clarifications contained in the Section 65B such as that the the Computer Output could be produced by a combination of computers, acting in succession etc as relating to dynamic creation of an electronic document from a data base and routing it through multiple devices onto a final visible form in the computer of the observer and thereafter its porting into a Printer.

i) Considering these interpretations, the Section 65B certification is a "matter of fact" certification to the effect that "What I saw is what I reproduced as a computer output faithfully" and this can be done by any person who is observing an electronic document in his computer and wants it to be produced as an evidence. It is not necessary that a document from yahoo website has to be certified only by a Yahoo server administrator. Similarly, a statement of account downloaded from an ICICI bank website need not be certified only by the ICICI Bank manager but by any person who can lawfully access the document in electronic form.

j) There is also an important distinction that "Content Owner" is different from "Content Viewer" and Section 65B is meant to be produced by a content viewer. On the other hand the content owner in respect of say a Bank statement is the official Bank manager and he can provide a print out as the owner of the content who understands the content and is considered as an "Expert" in the domain. Anybody else who views the document provides a Section 65B certificate that the print out (or a soft copy) is a faithful reproduction.

S. 73A. Proof as to verification of electronic signature.
In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct--
(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.
Explanation.-For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17of the Information Technology Act, 2000.
S. 81A. Presumption as to Gazettes in electronic forms.

S. 85A. Presumption as to electronic agreements.

S. 85B. Presumption as to electronic records and electronic signatures.

S. 85C Presumption as to Electronic Signature Certificates.

S. 88. And S 88A deals with Presumption as to telegraphic messages and to electronic messages.

S. 90A. Presumption as to electronic records five years old.

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

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

- **<u>Judicial Pronouncements on Relevance and Admissibility of Electronic Evidence</u>**

i. *Union of India and Ors. v. CDR Ravindra V. Desai*: (2018) 16 SCC 272.

The Court emphasised that non-production of a certificate Under Section 65B on an earlier occasion is a curable defect.

ii. *Sonu alias Amar v. State of Haryana:* (2017) 8 SCC 570,

The crucial test, as affirmed by Apex Court, is whether the defect of non production of certificate could have been cured at the stage of marking the document. If an objection was taken to the CDRs being marked without a certificate, the Court could have given the prosecution an opportunity to rectify the deficiency.

iii. *State vs. M.R. Hiremath* (01.05.2019 - SC) : 2019 (3) SCC (Cri.) 109

High Court erred in coming to the conclusion that the failure to produce a certificate Under Section 65B(4) of the Evidence Act at the stage when the charge-sheet was filed was fatal to the prosecution. The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise.

iv. *P. Gopalkrishnan vs. State of Kerala and Ors.* (29.11.2019 - SC) : AIR 2020 SC 1

The contents of the memory card/pen drive being electronic record must be regarded as a document. If the prosecution is relying on the same, ordinarily, the Accused must be given a cloned copy thereof to enable him/her to present an effective defence during the trial. However, in cases involving issues such as of privacy of the complainant/witness or his/her identity, the Court may be justified in providing only inspection thereof to the Accused and his/her lawyer or expert for presenting effective defence during the trial. The court may issue suitable directions to balance the interests of both sides.

v. Tomaso Bruno and Ram Singh [1985 Supp SCC 611]

It was held that electronic evidence is admissible and provisions under Sections 65-A and 65-B of the Evidence Act are by way of a clarification and are procedural provisions. If the electronic evidence is authentic and relevant the same can certainly be admitted subject to the Court being satisfied about its authenticity and procedure for its admissibility may depend on fact situation such as whether the person producing such evidence is in a position to furnish certificate under Section 65-B(4).

vi. Court in *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473: observed that electronic evidence by way of primary evidence was covered by Section 62 of the Evidence Act to which procedure of Section 65-B of the Evidence Act was not admissible. However, for the secondary evidence, procedure of Section 65-B of the Evidence Act was required to be followed and a contrary view taken in Navjot Sandhu [State (NCT of Delhi) v. Navjot Sandhu,: (2005) 11 SCC 600:] that secondary evidence of electronic record could be covered under Sections 63 and 65 of the Evidence Act, was not correct.

Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65-A, can be proved only in accordance with the procedure

prescribed Under Section 65-B. Section 65-B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer.

vii. In *Shafhi Mohammad vs. State of Himachal Pradesh,* (2018) 2 SCC 801, noticing the three Judge Bench Decision in Anvar P.V. have explained the said decision, holding the rigor of the rule there, that secondary evidence of electronic record can only be led subject to satisfaction of the requirements of Section 65-B(4), to be ameliorated in view of another three-Judge Bench Decision of their Lordships in Tomaso Bruno and another vs. State of Uttar Pradesh, (2015) 7 SC 178, and, laid down that in a case where electronic evidence is produced by a party, who is not in possession of the device, applicability of Sections 63 and 65 of the Evidence Act, cannot be held excluded. It is held there by their Lordships that the requirement of producing a certificate under Section 65-B(4), as a condition precedent to the leading of secondary evidence of electronic record, is attracted when such evidence is produced by a person, who is in control of the relative device, and, not when the device is with the opposite party.Thus the court clarified the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate Under Section 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies.

viii. *Arjun Panditrao Khodkar Vs. Kailash Kushanrao Gorantyal and Ors*.(14.07.2020)

Civil Appeal No.20825-20826 of 2017

With regard to the requirement of certificate under Section 65 B (4) the position was settled at rest in following terms

The required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4).

The judgment in *Tomaso Bruno* being per incuriam, does not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as *Shafhi Mohammad* and the judgment dated 03.04.2018 reported as (2018) 5 SCC 311, do not lay down the law correctly and are therefore overruled. I t is necessary to clarify what is contained in the last sentence in paragraph 24 of *Anvar P.V.*which reads as "…if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act…". This may

more appropriately be read without the words “under Section 62 of the Evidence Act,…”. With this minor clarification, the law stated in paragraph 24 of Anvar P.V. (supra) does not need to be revisited.

General directions are issued to cellular companies and internet service providers to maintain CDRs and other relevant records for the concerned period (in tune with Section 39 of the Evidence Act) in a segregated and secure manner if a particular CDR or other record is seized during investigation in the said period. Concerned parties can then summon such records at the stage of defence evidence, or in the event such data is required to cross-examine a particular witness. This direction shall be applied, in criminal trials, till appropriate directions are issued under relevant terms of the applicable licenses, or under Section 67C of the Information Technology Act,

Appropriate rules and directions should be framed in exercise of the Information Technology Act, by exercising powers such as in Section 67C, and also framing suitable rules for the retention of data involved in trial of offences, their segregation, rules of chain of custody, stamping and record maintenance, for the entire duration of trials and appeals, and also in regard to preservation of the meta data to avoid corruption. Likewise, appropriate rules for preservation, retrieval and production of electronic record, should be framed as indicated earlier, after considering the report of the Committee constituted by the Chief Justice’s Conference in April, 2016.

- **CONCLUSION**

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. Effective Legal enforcement of Cyberlaws requires a multipronged approach. No one strategy by itself is self sufficient or mutually exclusive to create effective enforcement results. To devise a well integrated action plan for cyber law enforcement is the need of the hour. It is imperative to spread greater awareness on the subject amongst general public and impart continuous training to the law enforcement personnel and forensic experts. Due measures to establish means and processes of evaluating new ICT developments and products including establishing accreditation agencies, certification policies, CERT, and procedures to enhance information security in the online world require strategic adoption . In addition to specific consumer protection initiatives, the private sector’s dedication and support for a secure Internet system is crucial to curbing unlawful conduct on the Internet. The public private participation and increased Corporate accountability and responsibility in maintaining security practices can assist in improved enforcement of cyber laws. In addition, global initiatives to harmonise cyber laws (in substantive and procedural spirit) will play a vital role in removing existing lacunae by crystallizing the laws of cyberspace. Participation of International organizations, professional & industry associations, law enforcement agencies, cyber law experts and other relevant bodies in creation of multilateral Treaties/Conventions and formulation of Code of Conduct for Cyberspace will assist in evolution of clear principles that will govern the cyberspace.