Unit 2: Internet crime and Act 2

Unit Structure

2.1 LEARNING OBJECTIVES

After study this student can learn:

- Internet crime and Act: A Brief History of the Internet,
- Recognizing and Defining Computer Crime,
- Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data,
- Indian IT ACT 2000.,
- Digital Evidences, Chain of Custody
- Intellectual Property in the Cyberworld

2.2 INTRODUCTION

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software licence is controversial and still evolving in Europe and elsewhere.

2.3 A BRIEF HISTORY OF THE INTERNET

According to Ministry of Electronic and Information Technology, Government of India

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

➢ Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

- Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

- Fraud:

Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

- Copyright:

The internet has made copyright violations easier. In early days of online communication, copyright violations was too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

- Defamation:

Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

- Harassment and Stalking:

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

➢ Freedom of Speech:

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

➢ Trade Secrets:

Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

➢ Contracts and Employment Law:

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

➢ Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notification on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application or any other document with any office, authority, body or agency owned or controlled by the suitable Government in e-form by means of such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

2.4 RECOGNIZING AND DEFINING COMPUTER CRIME

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

- What is the importance of Cyberlaw ?

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

- Does Cyberlaw concern me ?

Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyberlegal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

- Copyright Infringement through internet

Internet has become a breeding ground for violation of copyright. This mass misuse require more stringent laws.

2.5 CONTEMPORARY CRIMES

- Cyber Stalking: Challenges in Regulating Cyber Stalking At The Cyber Space

  What Is Cyber Stalking? There is no universal accepted definition of cyber stalking. The word stalking means ‘pursue stealthily' which refers that "harass obviously".

- Policy Hampering Illegal Data Entry Via Apps/Social Media
  How do you feel if someone unknowingly spies on your credit card number online? Won’t it get on your nerves? It definitely would come out as a blast of impulsiveness. Nobody, actually, likes to keep a watch on what indeed is so sensitive.

- Data Exclusivity A Necessary Evil
  Data Exclusivity refers to a practice whereby, for a fixed period of time, drug approval authorities do not allow the test data of the innovator company to be used to register equivalent generic version of that medicine.

- Computer Law
  Data Exclusivity Law: Data exclusivity is a matter of heated controversy now-a-days all over the world and a source of tussle between developing and developed countries

- Legal Dimensions of Information Technology - issues of copyright: It is related to the cyber world and the main focus is given on the issues such as the cyber crimes, right to information and the copyright issues.

- Digital Signatures: Digital Signatures have been provided for in the Information Technology Act, 2000, to bring about a minimum level of security in the increasing amount of data transfer over the Internet

- Electronic agents: Undoubtedly, the influences of IT (‘Information Technology’) have already invaded every corner of our daily lives. Nowadays, it is unimaginable if one determines not to relevant with this new technology at all.

- Data Theft in Cyber Space: This Article highlights the suseptibilty of data to theft in the digital age. It analyses as to what are the current provisions in the existing law on such theft and whether it can be brought under the ambit of the Indian Penal Code, 1860.
- Identity Theft: All across India, the fastest growing White Collar Crime in the nation has been identified as Identity Theft and its affecting each one of us in insidious ways
- Breach of privacy and Confidentiality: The article deals with Section 72 of the Information Technology Act, 2000 which speaks about penalty for Breach of Confidentiality and privacy
- Cyber Crimes and Cyber Law: Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology
- Cyber Terrorism and Various Legal Compliances: Terrorism is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience.
- Advertising - Its Evolution, Significance & Effects.
- Plagiarism: works created by other people is rightfully their intellectual property and if we use that work we are bound to
- Cyber Crimes and General Principles: Basic overview of the concept of cyber crimes and how the concept is different from the traditional principles of criminal law.
- Cyber Squatting- Clear and Present Danger: In the new e-economy it is commercially prudent for a company to have an easily traceable address in the cyber-space
- Cyber Crime And Law: contributes an understanding of the effects of negative use of Information technology
- Cyber Hacking: 'Hackers' are very intelligent people who use their skill in a constructive and positive manner

- Electronic Contract: traditional notion of contract formation, negotiating parties must come to a "meeting of the minds"
- The Bpo Strategy: Business Process Outsourcing (BPO) is a buzzword among the corporate in the world today.
- Need For Conversion Of The Convergence Bill: The Communication Convergence Bill, is on the verge of being enacted and changing the Indian communication machinery
- Data Safety And Privacy Protection: As the situation now warranty legislation of data protection in India, visitors to any website want reassurances that privacy rights
- The Menace of Cyber Crime: In the information age the rapid development of computers, telecommunications and other technologies has led
- Cyber-Elections: Its in-serverability has grown to such heights that perhaps George Bernard Shaw would have expressed as ‘Cyber-web here
- Defamation on the web: Who do you sue?: The law of defamation addresses harm to a person's reputation or good name through slander and libel.
- Internet telephony and related Issues: The focus of the article is to examine the impact of the proposed Communications Convergence.

2.6 INDIAN IT ACT 2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 May 2000. The bill was finalised by group of officials headed by then Minister of Information Technology PramodMahajan.

The original Act contained 94 sections, divided into 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of the Indian Penal Code, 1860, the Indian, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies.

A major amendment was made in 2008. It introduced Section 66A which penalized sending of "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced provisions addressing child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in LokSabha. The next day it was passed by the RajyaSabha. It was signed into law by President PratibhaPatil, on 5 February 2009.

Offences

List of offences and the corresponding penalties:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person 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	Imprisonment up to three years, or/and with fine up to ₹200,000

		or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	
66	Hacking with computer system	If a person 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 hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up

			to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images	If a person publishes or	Imprisonment up to

	containing sexual acts	transmits images containing a sexual explicit act or conduct.	seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	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. Any person who	Imprisonment up to three years, or/and with fine up to ₹200,000

		fails to comply with any such order shall be guilty of an offence.	
69	Failure/refusal to decrypt data	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. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.

70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

2.7 DIGITAL EVIDENCES & CHAIN OF CUSTODY

➢ **Section 66**

- In February 2001, in one of the first cases, the Delhi police arrested two men running a web-hosting company. The company had shut down a website over

non-payment of dues. The owner of the site had claimed that he had already paid and complained to the police. The Delhi police had charged the men for hacking under Section 66 of the IT Act and breach of trust under Section 408 of the Indian Penal Code. The two men had to spend 6 days in Tihar jail waiting for bail. BhavinTurakhia, chief executive officer of directi.com, said that this interpretation of the law would be problematic for web-hosting companies.

- In February 2017, M/s Voucha Gram India Pvt. Ltd, owner of Delhi based Ecommerce Portal www.gyftr.com made a Complaint with HauzKhas Police Station against some hackers from different cities accusing them for IT Act / Theft / Cheating / Misappropriation / Criminal Conspiracy / Criminal Breach of Trust / Cyber Crime of Hacking / Snooping / Tampering with Computer source documents and the Web Site and extending the threats of dire consequences to employees, as a result four hackers were arrested by South Delhi Police for Digital Shoplifting.

➢ **Section 66A**

- In September 2012, a freelance cartoonist AseemTrivedi was arrested under the Section 66A of the IT Act, Section 2 of Prevention of Insults to National Honour Act, 1971 and for sedition under the Section 124 of the Indian Penal Code. His cartoons depicting widespread corruption in India were considered offensive.
- On 12 April 2012, a Chemistry professor from Jadavpur University, AmbikeshMahapatra, was arrested for sharing a cartoon of West Bengal Chief Minister Mamata Banerjee and then Railway Minister Mukul Roy.The email was sent from the email address of a housing society. SubrataSengupta, the secretary of the housing society, was also arrested. They were charged under Section 66A and B of the IT Act, for defamation under Sections 500, for obscene gesture to a woman under Section 509, and abetting a crime under Section 114 of the Indian Penal Code.
- On 30 October 2012, a Puducherry businessman Ravi Srinivasan was arrested under Section 66A. He had sent tweet accusing Karti Chidambaram,

son of then Finance Minister P. Chidambaram, of corruption. Karti Chidambaram had complained to the police.

- On 19 November 2012, a 21-year-old girl was arrested from Palghar for posting a message on Facebook criticising the shutdown in Mumbai for the funeral of Bal Thackeray. Another 20-year-old girl was arrested for "liking" the post. They were initially charged under Section 295A of the Indian Penal Code (hurting religious sentiments) and Section 66A of the IT Act. Later, Section 295A was replaced by Section 505(2) (promoting enmity between classes). A group of Shiv Sena workers vandalised a hospital run by the uncle of one of girls.[19] On 31 January 2013, a local court dropped all charges against the girls.
- On 18 March 2015, a teenaged boy was arrested from Bareilly, Uttar Pradesh, for making a post on Facebook insulting politician Azam Khan. The post allegedly contained hate speech against a community and was falsely attributed to Azam Khan by the boy. He was charged under Section 66A of the IT Act, and Sections 153A (promoting enmity between different religions), 504 (intentional insult with intent to provoke breach of peace) and 505 (public mischief) of Indian Penal Code. After the Section 66A was repealed on 24 March, the state government said that they would continue the prosecution under the remaining charges.

➢ **Criticisms**

- **Section 66A and restriction of free speech**

  From its establishment as an amendment to the original act in 2008, Section 66A attracted controversy over its unconstitutional nature:

Section	Offence	Description	Penalty
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information	Imprisonment up to three years, with fine.

		which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	

In December 2012, P Rajeev, a RajyaSabha member from Kerala, tried to pass a resolution seeking to amend the Section 66A. He was supported by D. Bandyopadhyay, GyanPrakashPilania, BasavarajPatilSedam, Narendra Kumar Kashyap, Rama Chandra Khuntia and BaishnabCharanParida. P Rajeev pointed that cartoons and editorials allowed in traditional media, were being censored in the new media. He also said that law was barely debated before being passed in December 2008.

Rajeev Chandrasekhar suggested the 66A should only apply to person to person communication pointing to a similar section under the Indian Post Office Act, 1898. ShantaramNaik opposed any changes, saying that the misuse of law was sufficient to warrant changes. Then Minister for Communications and Information Technology KapilSibal defended the existing law, saying that similar laws existed in US and UK. He also said that a similar provision existed under Indian Post Office Act, 1898. However, P Rajeev said that the UK dealt only with communication from person to person.

- **Petitions challenging constitutionality**

  In November 2012, IPS officer Amitabh Thakur and his wife social activist Nutan Thakur, filed a petition in the Lucknow bench of the Allahabad High Court claiming that the Section 66A violated the freedom of speech guaranteed in the Article 19(1)(a) of the Constitution of India. They said that the section was vague and frequently misused.

  Also in November 2012, a Delhi-based law student, ShreyaSinghal, filed a Public Interest Litigation (PIL) in the Supreme Court of India. She argued that the Section 66A was vaguely phrased, as result it violated Article 14, 19

(1)(a) and Article 21 of the Constitution. The PIL was accepted on 29 November 2012.A similar petition was also filed by the founder of MouthShut.com, Faisal Farooqui, and NGO Common Cause represented by PrashantBhushan[28] In August 2014, the Supreme Court asked the central government to respond to petitions filed by Mouthshut.com and later petition filed by the Internet and Mobile Association of India (IAMAI) which claimed that the IT Act gave the government power to arbitrarily remove user-generated content.

- **Revocation by the Supreme Court**

  On 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India. But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deal with the procedure and safeguards for blocking certain websites.

- **Strict data privacy rules**

  The data privacy rules introduced in the Act in 2011 have been described as too strict by some Indian and US firms. The rules require firms to obtain written permission from customers before collecting and using their personal data. This has affected US firms which outsource to Indian companies. However, some companies have welcomed the strict rules, saying it will remove fears of outsourcing to Indian companies.

- **Section 69 and mandatory decryption**

  The Section 69 allows intercepting any information and ask for information decryption. To refuse decryption is an offence. The Indian Telegraph Act, 1885 allows the government to tap phones. But, according to a 1996 Supreme Court verdict the government can tap phones only in case of a "public emergency". But, there is no such restriction on Section 69.On 20 December 2018, the Ministry of Home Affairs cited Section 69 in the issue of an order authorising ten central agencies to intercept, monitor, and decrypt “any information generated, transmitted, received or stored in any computer.” While some claim this to be a violation of the fundamental right to

privacy, the Ministry of Home Affairs has claimed its validity on the grounds of national security.

- **The Concept of E-Evidence in India**

Due to enormous growth in e-governance throughout the Public & Private Sector and e-commerce activities Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. The government agencies are opening up to introduce various governance policies electronically and periodical filings to regulate and control the industries are done through electronic means. These various forms of Electronic Evidence/ Digital Evidence are increasingly being used in the judicial proceedings. At the stage of trial, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil law suit or conviction/acquittal of the accused. The Court continue to grapple with this new electronic frontier as the unique nature of e-evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences. The various categories of electronic evidence such as CD, DVD, hard disk/ memory card data, website data, social network communication, e-mail, instant chat messages, SMS/MMS and computer generated documents poses unique problem and challenges for proper authentication and subject to a different set of views.

The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Act was amended and the phrase “All documents produced for the inspection of the Court” were 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.

Under the provisions of Section 61 to 65 of the Indian Evidence Act, the word “Document or content of documents” have not been replaced by the word “Electronic documents or content of electronic documents”. Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has

omitted to use any word, the presumption is that the omission is intentional. It is well settled that the Legislature does not use any word unnecessarily. In this regard, the Apex Court in Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa held that "...Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislation; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily."

The intention of the legislature is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same. The Section 65B of the Evidence Act makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible. It provides: -

- Section 65B - Admissibility of Electronic Records

  Sec. 65B(1): Notwithstanding anything contained in this Act, any information contained in an electronic record -

  • which is printed on a paper, stored, recorded or

  • copied in optical or magnetic media

  • produced by a computer

  # shall be deemed to be also a document, if the conditions mentioned in this section are satisfied

  • in relation to the information and

  • computer in question and

  # shall be admissible in any proceedings, without further proof or production of the original,

  # as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

- Sec. 65B(2):

  # The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

  # Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer;

  # The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

  # Information reproduced is such as is fed into computer in the ordinary course of activity.

- Sec.65 B(3):

  The following computers shall constitute as single computer-

  # by a combination of computers operating over that period; or

  # by different computers operating in succession over that period; or

  # by different combinations of computers operating in succession over that period; or

  # in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

- Sec. 65B(4):

  Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things:

  - identifying the electronic record containing the statement and describing the manner in which it was produced;
  - giving the particulars of device
  - dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

This contention is further strengthened by the insertion words “Notwithstanding anything contained in this Act” to Section 65A & 65B, which is a non-obstante clause, further fortifies the fact that the legislature has intended the production or exhibition of the electronic records by Section 65A & 65B only. A non-obstante clause is generally appended to a Section with a view to give the enacting part of the Section, in case of conflict, an overriding effect over the provision in the same or other act mentioned in the non-obstante clause. It is equivalent to saying that despite the provisions or act mentioned in the non-obstante clause, the provision following it will have its full operation or the provisions embraced in the non-obstante clause will not be an impediment for the operation of the enactment or the provision in which the non-obstante clause occurs.

The aforesaid principles of interpretation with respect to the non-obstante clause in form of “Notwithstanding anything contained in this Act” is further supported by the Hon’ble Apex Court in Union of India and Anr., v. G.M. Kokil and Ors. observed “It is well-known that a non obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions.” Further, the Hon’ble Apex Court in the case cited as ChandavarkarSitaRatnaRao v. Ashalata S. Guram , explained the scope of non-obstante clause as “...It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation..."

- What Is the Chain of Custody in Computer Forensics?

  The chain of custody in digital forensics can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It indicates the collection, sequence of control, transfer, and analysis. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

- Why Is It Important to Maintain the Chain of Custody?

  It is important to maintain the chain of custody to preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible.

- Importance to the Examiner

  Suppose that, as the examiner, you obtain metadata for a piece of evidence. However, you are unable to extract meaningful information from it. The fact that there is no meaningful information within the metadata does not mean that the evidence is insufficient. The chain of custody in this case helps show where the possible evidence might lie, where it came from, who created it, and the type of equipment that was used. That way, if you want to create an exemplar, you can get that equipment, create the exemplar, and compare it to the evidence to confirm the evidence properties.

- Importance to the Court

  It is possible to have the evidence presented in court dismissed if there is a missing link in the chain of custody. It is therefore important to ensure that a wholesome and meaningful chain of custody is presented along with the evidence at the court.

- What Is the Procedure to Establish the Chain of Custody?

  In order to ensure that the chain of custody is as authentic as possible, a series of steps must be followed. It is important to note that, the more information a forensic expert obtains concerning the evidence at hand, the

more authentic is the created chain of custody. Due to this, it is important to obtain administrator information about the evidence: for instance, the administrative log, date and file info, and who accessed the files. You should ensure the following procedure is followed according to the chain of custody for electronic evidence:

- Save the original materials: You should always work on copies of the digital evidence as opposed to the original. This ensures that you are able to compare your work products to the original that you preserved unmodified.
- Take photos of physical evidence: Photos of physical (electronic) evidence establish the chain of custody and make it more authentic.
- Take screenshots of digital evidence content: In cases where the evidence is intangible, taking screenshots is an effective way of establishing the chain of custody.
- Document date, time, and any other information of receipt. Recording the timestamps of whoever has had the evidence allows investigators to build a reliable timeline of where the evidence was prior to being obtained. In the event that there is a hole in the timeline, further investigation may be necessary.
- Inject a bit-for-bit clone of digital evidence content into our forensic computers. This ensures that we obtain a complete duplicate of the digital evidence in question.
- Perform a hash test analysis to further authenticate the working clone. Performing a hash test ensures that the data we obtain from the previous bit-by-bit copy procedure is not corrupt and reflects the true nature of the original evidence. If this is not the case, then the forensic analysis may be flawed and may result in problems, thus rendering the copy non-authentic.

The procedure of the chain of custody might be different. depending on the jurisdiction in which the evidence resides; however, the steps are largely identical to the ones outlined above.

- What Considerations Are Involved with Digital Evidence?

  A couple of considerations are involved when dealing with digital evidence. We shall take a look at the most common and discuss globally accepted best practices.

  - Never work with the original evidence to develop procedures: The biggest consideration with digital evidence is that the forensic expert has to make a complete copy of the evidence for forensic analysis. This cannot be overlooked because, when errors are made to working copies or comparisons are required, it will be necessary to compare the original and copies.
  - Use clean collecting media: It is important to ensure that the examiner's storage device is forensically clean when acquiring the evidence. This prevents the original copies from damage. Think of a situation where the examiner's data evidence collecting media is infected by malware. If the malware escapes into the machine being examined, all of the evidence can become compromised.
  - Document any extra scope: During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. It is recommended that this information be documented and brought to the attention of the case agent because the information may be needed to obtain additional search authorities. A comprehensive report must contain the following sections:
    1. Identity of the reporting agency
    2. Case identifier or submission number
    3. Case investigator
    4. Identity of the submitter
    5. Date of receipt
    6. Date of report
    7. Descriptive list of items submitted for examination, including serial number, make, and model
    8. Identity and signature of the examiner
    9. Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files

10. Results/conclusions
11. Consider safety of personnel at the scene. It is advisable to always ensure the scene is properly secured before and during the search. In some cases, the examiner may only have the opportunity to do the following while onsite:
12. Identify the number and type of computers.
13. Determine if a network is present.
14. Interview the system administrator and users.
15. Identify and document the types and volume of media, including removable media.
16. Document the location from which the media was removed.
17. Identify offsite storage areas and/or remote computing locations.
18. Identify proprietary software.
19. Determine the operating system in question.
20. The considerations above need to be taken into account when dealing with digital evidence due to the fragile nature of the task at hand.

Check Your Progress 1:

1. List the history of Internet Crime.

2. How to recognise computer crime?

3. List out Contemporary Crimes.

4.Digital Evidences & Chain of Custody

2.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Refer the Topic no 2.2.
2. Refer the Topic no 2.4.
3. Refer the Topic no 2.5.
4. Refer the Topic no 2.7.