

Electronic Devices, Electronic Evidence, and Changing Trends

M.Suneel Kumar

XII ADJ, Vijayawada

Electronic Devices, Electronic Evidence, and Changing Trends

<i>I. Introduction, History, and Context of Electronic Devices.....</i>	<i>1</i>
<i>II. Definitions and Distinctions of Electronic Devices and Records.....</i>	<i>2</i>
<i>Meaning and Examples of Electronic Devices.....</i>	<i>2</i>
<i>III. Legal Definitions (IT Act, 2000).....</i>	<i>3</i>
<i>IV. Legal Definitions (D.P.D.P Act, 2023).....</i>	<i>4</i>
<i>Schedule of DPDP Act 2023.....</i>	<i>9</i>
<i>Distinction Between Electronic and Digital Records.....</i>	<i>10</i>
<i>V. Legislative Framework and Statutory Provisions.....</i>	<i>11</i>
<i>Legal Recognition (IT Act, 2000).....</i>	<i>11</i>
<i>Limitations and Exclusions (IT Act, 2000).....</i>	<i>12</i>
<i>VI. Provisions under BNSS (Section 530).....</i>	<i>12</i>
<i>VII. Admissibility of Electronic Evidence.....</i>	<i>14</i>
<i>Special Law Prevails Over General Law.....</i>	<i>14</i>
<i>Mandatory Requirement of Section 65-B Certificate (IEA).....</i>	<i>14</i>
<i>Primary Evidence Scope under BSA (Section 57).....</i>	<i>15</i>
<i>Admissibility Conditions under BSA (Section 63).....</i>	<i>16</i>
<i>Mandatory Certificate under BSA (Section 63(4)).....</i>	<i>17</i>
<i>VIII. Presumptions Regarding Electronic and Digital Records (BSA).....</i>	<i>17</i>
<i>IX. Collection and Preservation of Electronic Evidence.....</i>	<i>19</i>
<i>Critical Steps to Prevent Data Loss.....</i>	<i>19</i>

<i>Forensic Methods of Preservation :.....</i>	<i>20</i>
<i>Problems in Preservation.....</i>	<i>21</i>
<i>X. Appreciation of Specific Electronic Evidence Types.....</i>	<i>21</i>
<i>Email and Electronic Records.....</i>	<i>21</i>
<i>Instant Messages (IM) and WhatsApp.....</i>	<i>24</i>
<i>Tape Recorded Conversation and CCTV.....</i>	<i>26</i>
<i>IP Address as Evidence.....</i>	<i>27</i>
<i>Call Data Records (CDRs).....</i>	<i>27</i>
<i>Compact Disc's.....</i>	<i>28</i>
<i>Bankers' Books Evidence.....</i>	<i>29</i>
<i>XI. Authenticity, Characteristics, and Challenges of Electronic Evidence.....</i>	<i>30</i>
<i>Trustworthiness and Authenticity.....</i>	<i>30</i>
<i>Components Subject to Authenticity Issues.....</i>	<i>30</i>
<i>Challenges to Authenticity in Court.....</i>	<i>31</i>
<i>Fundamental Characteristics and Technical Challenges.....</i>	<i>31</i>
<i>XII. Modifications to the Indian Penal Code (IPC) (1860).....</i>	<i>32</i>
<i>XIII. Conclusion.....</i>	<i>33</i>

Electronic Devices, Electronic Evidence, and Changing Trends

I. Introduction, History, and Context of Electronic Devices

The origin of the programmable computer is attributed to **Charles Babbage**, an English mechanical engineer and polymath, who is considered the "father of the computer" for conceptualising and inventing the first mechanical computer in the early 19th century. Over the past 200 years, computer technology has reached all walks of human life. We are now in the era of the virtual reality world, where the use of electronic devices has become **indispensable and a part of human life**. This pervasive use forced the enactment of the **Information Technology (IT) Act in 2000**, which amended many provisions in other laws. The IT Act 2000 underwent amendments in 2015. The significant "**amendment**" to the Information Technology Act in 2015 was not a legislative act, but the Supreme Court's landmark judgment in ***Shreya Singhal V. Union Of India AIR 2015 S.C 1523***, which declared Section 66A of the Act unconstitutional. However, there were several administrative amendments made in 2015 to various rules under the Act. **Recently, the Digital Personal Data Protection (DPDP) Act 2023** was also enacted to protect personal data. For breaches, the penalties contemplated are up to **two hundred and fifty crore rupees**.

The world is now divided by a **digital divide**, meaning there is a gap (like "haves and have-nots") between those who have access to technology, the internet, and digital literacy training, and those who do not. This divide affects all generations, both rural and urban communities, and a wide variety of industries and sectors.

Despite 25 years having lapsed, and the extensive use of electronic devices in all aspects of life, people are **still illiterate with regard to the**

maintenance and management of electronic devices and evidence. When electronic devices became integral to our lives, the nature of crime also changed its face. While the purpose of any new invention is to make human life more comfortable and things easier, using these new technologies carries repercussions. The judges deciding disputes must know everything about electronic records, as they are **easy to manipulate and vulnerable to tampering**. The recent pandemic highlighted the importance of using Information and Communication Technology (ICT) in the judicial system, moving society into the flow of modern civilised society. Specific provisions regarding electronic records were incorporated into recently introduced criminal laws.

II. Definitions and Distinctions of Electronic Devices and Records

Meaning and Examples of Electronic Devices

Electronic devices are hardware that control the flow of electric currents to process, control information, and systems, by using transistors and Integrated Circuits (IC's). They manipulate and process information by controlling the flow of electric charge through components. They differ from electrical devices, which typically perform simpler tasks like heating or mechanical work, often using passive components like resistors. The controlled flow of electrons is used to accomplish specific functions, ranging from simple tasks to complex operations.

Examples of Electronic Devices:

- **Broad Categories:** Computers, smartphones, CCTV, and Internet of Things (IoT) gadgets.
- **Consumer Electronics:** Smartphones, laptops, televisions, and tablets.
- **Medical Devices:** Pacemakers, insulin pumps, and deep-brain stimulators.

- **Industrial and Computing:** Microprocessors, integrated circuits, vending machines, and ATMs.
- **Home Appliances:** Washing machines and other modern kitchen appliances.
- **Communication Devices:** Devices used for audio, video, or text communication.

III. Legal Definitions (IT Act, 2000)

- **Electronic Record (S. 2(t)):** Data, record or data generated, image or sound stored, received, or sent in an electronic form or micro film or computer-generated micro fiche.
- **Electronic Form (of Information) (S. 2(r)):** Any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche, or similar device.
- **Electronic Form Evidence (S. 79A Explanation):** Any information of **probative value** that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, and digital fax machines.
- **Data (S. 2(o)):** A representation of information, knowledge, facts, concepts, or instructions prepared in a formalised manner, intended to be processed, being processed, or having been processed in a computer system or computer network. It may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

- **Information (S. 2(v)):** Includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.
- **Intermediary (S. 2(w)):** Any person who, on behalf of another, receives, stores, or transmits that record or provides any service with respect to that record. This 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.
- **Digital Signature (S. 2(p)):** Authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.
- **Electronic Signature (S. 2(ta)):** Authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

IV. Legal Definitions (D.P.D.P Act, 2023)

- **S.2(b) “automated”** means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data.
- **S.2(i) “Data Fiduciary”** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;
- **S.2(j) “Data Principal”** means the individual to whom the personal data relates and where such individual is
 - (i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on her behalf.

- **S.2(m) “digital office”** means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;
- **S.2(n) “digital personal data”** means personal data in digital form;
- **S.2(t) “personal data”** means any data about an individual who is identifiable by or in relation to such data;
- **S.(u) “personal data breach”** means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;
- **(y) “she”** in relation to an individual includes the reference to such individual irrespective of gender;

Data theft

Data Theft refers to the illegal act of stealing or copying sensitive, confidential, or personal information without the owner’s knowledge or consent. It often involves unauthorized access to databases, networks, or devices to obtain information for financial, competitive, or malicious purposes.

Examples of Stolen Data: Personal identification details (e.g., Aadhaar numbers), financial information (credit card numbers, bank details), corporate secrets, intellectual property, and health records.

Personal Data Theft

Involves stealing information such as names, addresses, phone numbers, and financial information to commit identity theft or fraud.

Example: Hackers steal credit card information and use it to make unauthorized purchases.

Corporate Data Theft:

Targeting companies to steal trade secrets, intellectual property, customer databases, or other confidential business information.

Example: Competitors hacking into a business's system to obtain proprietary product designs or business strategies.

Financial Data Theft:

Involves the theft of sensitive financial information like credit card numbers, bank account details, and transaction histories.

Example: Cybercriminals hack into an online banking system to steal funds from user accounts.

Health Data Theft:

Stealing sensitive health records and insurance information, often to commit identity theft or fraud.

Example: Hackers breach hospital databases to steal patients' medical histories.

Government and Military Data Theft:

Involves hacking into government databases or military systems to access classified information.

Example: Cyber espionage by foreign actors seeking to gather intelligence or disrupt national security.

Common Methods Used in Data Theft**Phishing:**

A form of social engineering where attackers trick individuals into providing sensitive information through fake emails, websites, or messages. Often used to steal login credentials or financial details.

Example: A user receives a fake email that appears to be from their bank, asking them to verify their account details by entering their credentials on a malicious site.

Malware:

Malicious software such as viruses, ransomware, or spyware can infect a system to extract sensitive data.

Example: A Trojan horse program disguises itself as legitimate software but collects personal or financial data once installed on the user's device.

Insider Threats:

Employees or insiders with access to sensitive data can intentionally or unintentionally steal or leak confidential information.

Example: A disgruntled employee downloads a customer database and sells it to a competitor.

SQL Injection:

Attackers exploit vulnerabilities in a website's database management system to execute SQL queries that allow unauthorized access to data.

Example: A hacker uses SQL injection to access usernames, passwords, and financial information stored in a website's database.

Man-in-the-Middle (MitM) Attacks:

Cybercriminals intercept communication between two parties to steal sensitive information, often during online transactions.

Example: A hacker intercepts data being transmitted between a user and a banking website, stealing login credentials.

Physical Theft:

Data can be stolen through the theft of physical devices like laptops, smartphones, or storage media (USB drives) that contain sensitive information.

Example: A stolen laptop containing confidential business data that isn't encrypted or password-protected.

Impact of Data Theft

Personal Impact:

Identity Theft: Stolen personal data can be used to create fake identities, access bank accounts, or commit fraud.

Financial Loss: Victims of data theft can experience direct financial losses from unauthorized transactions or account takeovers.

Emotional Distress: Loss of privacy, fear of future attacks, and reputational damage can lead to anxiety and emotional distress for victims.

Impact on Businesses:

Reputational Damage: Businesses that suffer data breaches often lose the trust of customers and partners, leading to a loss of business.

Financial Losses: Costs related to responding to the breach, such as compensating victims, upgrading security systems, and facing potential fines.

Legal Consequences: Companies can be sued for negligence or face regulatory penalties if they fail to protect sensitive customer data.

National Security Risks:

When government or military data is stolen, it can pose serious risks to national security. For example, breaches of defense systems or diplomatic communications can compromise a nation's safety.

Industry-Specific Risks:

In sectors like healthcare or finance, data theft can lead to significant regulatory consequences. Organizations in these industries must comply with stringent data protection laws (e.g., HIPAA in healthcare, PCI DSS in finance), and data theft can lead to hefty fines and regulatory action.

Notable Data Theft Incidents in India

Aadhaar Data Leak (2018):

In 2018, reports emerged that personal information of over a billion Indian citizens, collected under the Aadhaar system, was accessible to hackers. Although the government denied large-scale data breaches, concerns about the security of Aadhaar data grew.

Zomato Data Breach (2017):

Zomato, a popular food delivery platform, suffered a breach where the personal data of 17 million users, including names, email addresses, and hashed passwords, was stolen and listed for sale on the dark web.

Mobikwik Data Breach (2021):

Personal information, including KYC data of millions of Mobikwik users, was allegedly leaked online. The breach included details like phone numbers, addresses, Aadhaar cards, and other sensitive information.

Schedule of DPDP Act 2023

Section 33(1)

Sl No	Breach of provisions of this Act or rules made thereunder	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (5) of section 8.	May extend to two hundred and fifty crore rupees.
2	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (6) of section 8.	May extend to two hundred crore rupees.

3	Breach in observance of additional obligations in relation to children under section 9.	May extend to two hundred crore rupees.
4	Breach in observance of additional obligations of Significant Data Fiduciary under section 10.	May extend to one hundred and fifty crore rupees.
5	Breach in observance of the duties under section 15	May extend to ten thousand rupees.
6	Breach of any term of voluntary undertaking accepted by the Board under section 32.	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7	Breach of any other provision of this Act or the rules made thereunder	May extend to fifty crore rupees.

Distinction Between Electronic and Digital Records

The terms "electronic record" and "digital record" are often used interchangeably, but they have **distinct meanings**. Understanding these differences is essential in fields like information management, legal compliance, and technology.

Feature	Electronic Record	Digital Record
Origination	Can originate from both analog and digital sources (e.g., a paper document scanned into a PDF).	Originate inherently in a digital format (e.g., a spreadsheet created in Excel, digital art).

Format	Includes both scanned versions of physical documents and digitally born content.	Specifically refers to content created and stored in a digital format.
Metadata	May include basic metadata (file type, size, date modified).	Often includes extensive metadata , including authorship, creation date, version history, and digital signatures for authenticity.
Transformation	Analog records can be transformed through digitization (e.g., scanning).	Are inherently digital and do not require transformation from an analog state.

Digital record is not defined anywhere in the IT Act or the BSA. Generally, information stored or transmitted electronically is said to be "digital" because it has been broken down into digits, i.e., binary units of 0s and 1s, representing "information of probative value that is stored or transmitted in binary form". **In a nutshell, while all digital records are electronic records, not all electronic records are digital.**

V. Legislative Framework and Statutory Provisions

Legal Recognition (IT Act, 2000)

Section 4 of the IT Act gave legal recognition to electronic records. Where any law requires information to be in writing, typewritten, or printed form, that requirement is deemed satisfied if such information or matter is:

1. Rendered or made available in an electronic form; **and**

2. Accessible so as to be usable for a subsequent reference. This provision enables the public to use it in their day-to-day activities.

Limitations and Exclusions (IT Act, 2000)

- **Right to Insist (Section 9):** Nothing in Sections 6, 7, and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central or State Government, or any authority established by or under any law or controlled or funded by them, should accept, issue, create, retain, and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.
- **Excluded Documents (Section 1(4) and Schedule 1):** The IT Act is **not applicable** to five categories of documents:
 1. Negotiable instruments other than the cheque.
 2. A Power of Attorney Act.
 3. A trust as defined under the Indian Trust Act.
 4. A Will as defined under clause (h) of section 2 of the Indian Succession Act, including any other testamentary disposition.
 5. Any contract for the sale or conveyance of immovable property, or any interest in such property.

VI. Provisions under BNSS (Section 530)

The Bharatiya Nagarik Suraksha Sanhita (BNSS) also recognised the use of electronic records. Section 530 allows all trials, inquiries, and proceedings—including issuance, service, and execution of summons and warrants; examination of witnesses; recording of evidence; and all appellate or other proceedings to be held in **electronic mode**, by use of electronic communication

or audio-video electronic means. The legislature intended to use ICT to the maximum extent to shorten delays in judicial proceedings and ensure court proceedings are not stalled.

- **Audio-Video Electronic Means (S. 2(a)):** Shall include the use of any communication device for video conferencing, recording processes of identification, search and seizure or evidence, transmission of electronic communication, and for such other purposes as the State Government may provide by rules.
- **Electronic Communication (S. 2(i)):** The communication of any written, verbal, pictorial information, or video content transmitted (from person to person, device to device, etc.) by means of an electronic device, including a telephone, a mobile or cellular phone, a computer, or audio-video players and cameras.

Directions while recording evidence through video conference. **Raj Kumar Alias Bheema Vs. State Of Nct Of Delhi, AIROnline 2025 SC 1085**

“48. . Therefore, we hereby clarify and direct that in every case where, it is proposed to record the statement of a witness over video conferencing and any previous written statement of such witness or a matter in writing is available and the party concerned is desirous of confronting the witness with such previous statement/matter in writing, the trial Court shall ensure that a copy of the statement/document is transmitted to the witness through electronic transmission mode and the procedure provided under Section 147 and Section 148 of the Bharatiya Sakshya Adhiniyam (corresponding Section 144 and Section 145 of the Evidence Act) is followed in the letter and spirit, so as to safeguard the fairness and integrity of the trial.”

VII. Admissibility of Electronic Evidence

Special Law Prevails Over General Law

The admissibility of secondary evidence pertaining to an electronic record is **wholly governed by Sections 65-A and 65-B** of the Indian Evidence Act (IEA). The evidence relating to electronic record is a special provision. The general law on secondary evidence under Section 63 read with Section 65 of the Evidence Act shall yield to this special provision, based on the principle *Generalia specialibus non derogant*. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated in *State (NCT of Delhi) v. Navjot Sandhu* (2005), does not lay down the correct legal position and has been overruled.

Mandatory Requirement of Section 65-B Certificate (IEA)

The certificate required under **Section 65-B(4) is a condition precedent to the admissibility of evidence by way of electronic record** **When it is secondary evidence**. Oral evidence in the place of such certificate cannot possibly suffice, as Section 65-B(4) is a mandatory requirement of the law. To hold otherwise would render Section 65-B(4) otiose.

- **Current Authoritative Stance:** The Supreme Court in **Chandrabhan Sudam Sanap v. The State Of Maharashtra AIR 2025 S.C1103** admissibility of CCTV footage:- by producing CCTV footage, prosecution sought to prove that the accused was last seen at railway station with deceased who was allegedly murdered by him-objection regarding absence of certificate u/s65-B of evidence Act was raised at the earliest point of time, CCTV footage was not admissible in evidence since said certificate is a condition precedent to admissibility of evidence in the nature of electronic evidence since said certificate is a condition precedent to admissibility of evidence in the nature of electronic record even otherwise prosecution has failed to answer issues regarding life time

of CCTV footage in DVR-II being 12 days, absence of both the accused and deceased in the same footage etc, **renders electronic records inadmissible.**

- **Application:** If the electronic evidence (such as photographs or videos from mobile phones) is a **copy of the original**, i.e., secondary evidence, the requirement of Section 65-B arises. An electronic record by way of secondary evidence (CD, VCD, chip, etc.) shall not be admitted unless the requirements under Section 65-B are satisfied, and it must be accompanied by the certificate obtained at the time of taking the document. For photographs, the original device used to capture them has to be produced; otherwise, the copy must be produced along with a 65-B certificate.

Primary Evidence Scope under BSA (Section 57)

The BSA extends the scope of primary evidence by considering the observations of the Apex Court and developments in ICT.

- **Multiple Files (Explanation 4):** Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, **each such file is primary evidence.**
- **Proper Custody (Explanation 5):** An electronic or digital record produced from **proper custody** is primary evidence unless it is disputed.
- **Video Recording Transmission (Explanation 6):** Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, **each of the stored recordings is primary evidence.**
- **Multiple Storage Spaces (Explanation 7):** Where an electronic or digital record is stored in multiple storage spaces in a computer resource, **each**

such automated storage, including temporary files, is primary evidence.

Admissibility Conditions under BSA (Section 63)

Section 61 confirms that nothing in the Adhiniyam shall apply to deny the admissibility of an electronic or digital record on the ground that it is such a record, and it shall have the same legal effect, validity, and enforceability as other documents, subject to Section 63. The contents of electronic records may be proved in accordance with the provisions of Section 63.

Any information contained in an electronic record (the "computer output"), which is printed, stored, recorded, or copied in optical or magnetic media or semiconductor memory, shall be deemed to be a document and admissible if the conditions in Section 63(2) are satisfied.

The conditions for the computer output are:

1. The device was used **regularly** to create, store, or process information for regular activity by the person having lawful control.
2. Information of that kind was **regularly fed** into the device in the ordinary course of the said activities.
3. Throughout the material part of the said period, the device was **operating properly** (or, if not, the malfunction did not affect the accuracy of the contents).
4. The information in the electronic record reproduces or is derived from such information fed into the device in the ordinary course of the said activities.

If the function was performed by means of one or more devices (in standalone mode, on a computer system, network, resource, or through an intermediary),

all the devices shall be treated as constituting a single computer or communication device.

Mandatory Certificate under BSA (Section 63(4))

A **certificate** must be submitted **along with the electronic record at each instance** where it is being submitted for admission. The certificate, purporting to be signed by a person in charge or management or an expert, must:

- Identify the electronic record and describe the manner of its production.
- Give sufficient particulars of any device involved to show it was produced by a computer or communication device.
- Deal with any of the matters related to the conditions mentioned in S.63(2).

VIII. Presumptions Regarding Electronic and Digital Records (BSA)

The BSA provided specific provisions with regard to presumptions of electronic or digital record or signatures.

Presumption	Provision (BSA)	Details
Electronic Signature	S.66	Must be proved to be the subscriber's signature, except for a secure electronic signature.
Digital Signature	S.73	The Court may direct the purported person or the Certifying Authority to produce the Digital Signature Certificate to ascertain authenticity.
Official Gazettes	S.81	Court shall presume genuineness if the record

		purports to be the Official Gazette, is kept substantially in the required form, and is produced from proper custody .
Electronic Agreements	S.85	Court shall presume that the agreement was concluded by affixing the electronic/digital signatures of the parties.
Secure Records/Signatures	S.86	Secure records are presumed not to have been altered since the secure status relates. Secure electronic signatures are presumed to be affixed by the subscriber with the intention of signing or approving the record.
Electronic Signature Certificates	S.87	Court shall presume the information listed in the certificate is correct, unless contrary is proved, except for unverified subscriber information.
Electronic Messages	S.90	Court may presume that an electronic message corresponds with the message fed into the computer for transmission, but shall not make any presumption as to the person who sent the message .
Old Records	S.93	Where an electronic record is five years old and produced from proper custody, the Court may presume the electronic signature was affixed by the purported person or someone authorised.

Note: For Sections 81 and 93, custody is proper if records are in the place in which, and looked after by the person with whom such document is required to be kept.

IX. Collection and Preservation of Electronic Evidence

The nature of electronic evidence is **highly volatile**, making it important to handle the evidence and cases involving it very carefully. The collection process involves using forensic tools to capture data without altering it, while preservation ensures its integrity and authenticity for legal proceedings.

Critical Steps to Prevent Data Loss

Time is highly important in preserving digital evidence. A series of steps must be followed, as even a small inattentive move could lead to a loss of evidence and the break of a case:

1. **Do not change the current state of the device:** If the device is OFF, keep it OFF; if ON, keep it ON. Call a forensics expert before doing anything.
2. **Power down mobile phones:** If a mobile phone is ON, power it down to prevent any data wiping or overwriting due to automatic booting. Do not charge it if it is uncharged.
3. **Secure the device:** Do not leave the device unattended in an open area or unsecured place. Document where the device is, who has access, and when it is moved.
4. **Do not plug any external storage media** (memory cards, USB drives) into the device.
5. **Do not copy anything to or from the device:** Copying will cause changes in the slack space of the memory.

6. **Document the evidence:** Take pictures of the evidence from all sides to ensure it has not been tampered with until forensic experts arrive.
7. **Know the login credentials** (PIN/Password Pattern) and share them with the forensic experts.
8. **Do not open anything** (pictures, applications, or files) on the device, which may cause losing the data or memory being overwritten.
9. **Trust only certified Forensics experts:** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained persons may cause the deletion of data or the corruption of important information.
10. **Do not Shut down a computer; Hibernate it:** If required, hibernation preserves the contents of the volatile memory until the next system boot.

In criminal matters, when seizing electronic evidence, the evidence collector should **always take a backup and keep it sealed**. The date and time shown in the computer, the version of the operating system, and any software installed and used to examine the computer must be recorded. Hard disks, even if used just once and wiped clean, will be considered electronic records.

Forensic Methods of Preservation :

1. **Drive Imaging:** An analyst creates a **bit-by-bit duplicate (an image)** of the drive. Forensic analysis must **never** be performed on the original media. A **write blocker** (hardware or software) should be used to create the image to facilitate legal defensibility. Even wiped drives can retain important and recoverable data.
2. **Hash Values:** Cryptographic hash values (like MD5, SHA1) are generated during imaging. These fixed-length strings are unique to the file being

hashed. They are critical as they verify the **authenticity and integrity** of the image as an exact replica of the original media. If the hash values of the image and the original evidence do not match, it may raise concerns about tampering. Altering even the smallest bit of data will generate a completely new hash value.

3. **Chain of Custody (CoC):** Forensic investigators must document all steps conducted during the transfer of media on CoC forms, capturing signatures, date, and time upon media handoff. CoC demonstrates that the image has been under known possession. **Any lapse in the CoC nullifies the legal value** of the image and the analysis. If digital media is evidence of a crime, it should be immediately quarantined and put under the CoC.

Problems in Preservation

The highest risk is **legal admissibility**. The risk of vital evidence destruction grows with the amount of time that has elapsed since the incident took place, especially if the media is still in service.

X. Appreciation of Specific Electronic Evidence Types

Email and Electronic Records

An Email downloaded and printed from the Email account of the person can be proved by virtue of **Section 65B read with Section 88A of the IEA, 1872**. The testimony of the witness who carried out the procedure to download and print the same is sufficient to prove the electronic communication. However, in the absence of a certificate along with an email printout, **it is not admissible**.

- **Presumption on Sender Identity:** While the Court may make an assumption about the content of the message itself from the message at

the Mail Server, the Court **shall not make any assumption as to the person by whom such message was sent** (Section 88A).

- **Agreements:** In the absence of a signed agreement between the parties, an enforceable understanding could be inferred from the exchange of emails, letters, telex, telegrams, and other means of telecommunications, provided they were duly approved and signed by the parties.
- The Hon'ble High Court of Calcutta in **Abdul Rahaman Kunji Vs. The State of West Bengal , MANU/WB/0828/2014.**

The facts of the case are that Abdul Rahaman Kunji and seven others were accused of conspiring to abduct Partha Roy Barman and hold him for ransom. It was alleged that the conspiracy was hatched by Abdul Rahaman Kunji and Aftab Ahmed Ansari in Dubai. The particulars of the conspiracy were chalked out by the conspirators including Abdul Rahaman Kunji and finalized in a flat at 21B, Gorachand Lane. The victim was abducted and a ransom of Rs 1.5 crores was demanded. The accused were charged under Sections 364A (kidnapping for ransom) and 120B (criminal conspiracy) of the IPC.

The prosecution relied heavily on the emails exchanged between the conspirators, including Abdul Rahaman Kunji and Asif Reza Khan, to establish the conspiracy. The emails provide evidence of the plan to abduct the victim and hold him for ransom. The emails also indicate the initial target was "Haldiram" and was later changed to "Khadim Jutawala". The prosecution was able to establish that Akib Ali was the originator of 23 out of the 25 emails produced by them and that the contents of these emails are admissible in evidence under section 65B of the Evidence Act. Therefore, the Court relied on the emails as evidence to convict the accused

while deciding the admissibility of Email held that an Email downloaded and printed from the Email account of the person can be proved by virtue

of Section 65B read with Section 88A of the IEA, 1872. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication. In **Indian Micro Electronics (P) Ltd. Vs. Chandra Industries and Ors, 2015 VIAD (Delhi)** 52.it was held , that in absence of a certificate along with an email printout, it is not admissible.

The Court also observed that with respect to the contents of the message, the Court may make an assumption about the message itself from the message at the Mail Server but court shall not make any assumption as to the person by whom such message was sent.¹ Section 88A, of the Indian Evidence Act, 1872.

Section 88A of the Evidence Act allows the Court to presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed in the computer for transmission. However, the Court cannot draw any presumption about the person who sent the message. Besides, no presumption can be drawn about the person who has sent such a message. Therefore, even if we accept the fact that these e-mails have been downloaded as stated by the Webel expert or sent by using the e-mail address of Akib Ali, it was necessary for the prosecution to prove that Akib Ali was in fact the originator of these e-mails.

Babu Ram Aggarwal & Anr. vs Krishan Kumar Bhatnagar & Ors.
<https://indiankanoon.org/doc/135497619/>

The plaintiffs are seeking specific performance from the defendants to transfer a share in the property via sale deeds. The property was originally owned by the father of the defendants, who passed it on to his three sons through a registered will. After a series of agreements and settlements,

the plaintiffs approached the defendants to purchase a share of the property, which was agreed to, but the transfer has yet to take place.

The Delhi High court examined certain emails in the context of a property sale agreement case, and it concluded that these emails did not provide sufficient evidence of consent or authority for the sale. Additionally, the court pointed out several specific issues with the emails, such as lack of statements confirming the identity of the email senders, lack of evidence of email delivery, and uncertainty regarding the references cited in the emails

Instant Messages (IM) and WhatsApp

Electronic messages sent via IM services and messengers are also electronic records within the meaning of the IEA, 1872. However, **without the certificate compliance (S. 65B), such messages are not admissible.**

AIROnline 2025 KAR 1289 H.N.Vs H.N Mallesappa (Karnataka High Court)

S. 65B Electronic evidence WhatsApp messages and bank statements
Admissibility:- In a suit for recovery of money, plaintiff had relied on WhatsApp messages and bank statements to prove loan transaction - Compliance under S. 65B(4) was required only when secondary copies of an electronic record are relied upon - Primary electronic records could be relied upon even without a certificate - In the instant case, S. 65B certificate produced by plaintiff had remained unchallenged and combined with uncontroverted bank transfers, electronic evidence was admissible and sufficient to prove acknowledgment of debt - Defendant had failed to rebut or prove repayment - Decree of Trial Court against defendant was proper. (Para No(s) 11)

In Karan Mathur v State (NCT of Delhi), 2017 Indlaw DEL 910. It was held that Electronic messages being presented at the stage of bail hearing have also been held to be of relevance to either grant or refuse bail to an accused.

WhatsApp chats and emails are admissible in evidence during trial. Electronic messages presented at the stage of bail hearing have also been held to be of relevance to either grant or refuse bail.

The Punjab & Haryana High Court held that **WhatsApp chats shall have no evidentiary value** until a certificate is produced under **Section 65B(4)**.

In Neeraj Kumarpal Shah v Dinesh Shivanna and others ,2017 Indlaw GUJ 1047 it was held Electronic messages sent via IM services and messengers are also electronic records within the meaning of the IEA,1872. However, without the certificate compliance, such messages are not admissible.

Challenges and Solutions for WhatsApp:

- **Blue Ticks:** The Bombay High Court observed that a blue tick appearing after a message is sent via WhatsApp is viewed as **factual verification** that the recipient had gotten and opened that notice. However, users can hide their blue ticks (disable read receipts). If the recipient has a track record of responding to messages without displaying blue ticks, it may be reasonably inferred that their consistent conduct indicates they have indeed seen and received the message in question.
- **Exported Messages:** Challenges include the **exclusion of media** (photos/videos) and the **lack of identity verification**, as the transcript only displays the name saved in the contact book, not the phone number. They also do not highlight the phone numbers of either party.
- **Forensic Solutions:** The safest course of action is to **produce the original WhatsApp messages** as they appear on the witness' phone, as courts cannot rely on screenshots alone due to the possibility of fabrication. Digital forensic techniques can analyze image file structure, metadata, compression artifacts, and other technical aspects to identify signs of manipulation or tampering.

Tape Recorded Conversation and CCTV

Tape recorded conversations are admissible provided the voice of the people can be recognized, the recording is relevant, and the **possibility of tampering is done away with**. Transcriptions of tape recorded conversation without the original recording put to source and authentication test are **not admissible**. Voice identification should be conducted via due process, such as mixing of samples and not telling the witness about them at all.

AIR 2017 SC 3227 Vikram Singh Alias Vicky Walia Vs State of Punjab

S.65B Tape-recorded conversation Admissibility in evidence - Tape-recorded conversation not a secondary evidence which requires certificate under S. 65-B, since it was original cassette by which ransom call was tape-recorded - Conversation recorded containing ransom calls relevant under S. 7 and primary evidence relied on by complainant - Is admissible in evidence. (Para No(s) 24)

The Supreme Court held that the computer generated electronic records in evidence are admissible if proved in the manner specified by **Section 65B**. The Delhi High Court has held that CCTV footage recorded directly onto a hard disk that is properly numbered and serialised is **primary evidence** and may not require a Section 65B certificate.

InTomso Bruno and anr. V. State of U.P, AIR 2015 SC (SUPP) 412.

The Hon'ble Supreme Court has held that the computer generated electronic records in evidence are admissible at a trial if proved in the manner specified by section 65B of the IEA,1872. The court pointed CCTV footage in the case was the best evidence and that non-admission of the footage at the trial stage was faulty. The Court also highlighted the importance of a certificate under section 65B as crucial to often proving the guilt of an accused.

The Delhi High Court has gone on to say that CCTV footage is recorded directly by way of such programming onto a hard disk directly. This evidence is primary i.e. the hard disk. As per section 60 of the IEA,1872, when the CCTV clip is played, the court becomes witness to the act although the crime was committed

prior in time **Kailash H. Vs. Suresh Chandra, 2011 LawSuit (MP) 598.**

However, it was subject to integrity checks based on testimonies of experts but it leads to the belief that CCTV footage produced directly on the hard disk that it is programmed to store it on by properly numbering and serializing is primary evidence and does not require Section 65B certificate.

Syed Asifuddin & Ors. Vs State of A.P., 2005 CriLJ 4314 A cellphone has also been deemed to be a computer under the IT Act, 2000. Hence, in all cases, printouts or documents so produced by this computer are also 'electronic records'.

IP Address as Evidence

An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number. Proving guilt solely by way of IP Address and internet connection mapping has **not been held to be sufficient**; it can prove the incident origin but not the person who committed an act.

Call Data Records (CDRs)

CDRs are **inadmissible without a section 65B certificate**. CDRs aid in preliminary investigation but cannot be taken as conclusive evidence because of issues like the handset being with someone else, lack of 65B certification, SIM card cloning, or mobile number spoofing. The Supreme Court relied on the proposition that CDRs cannot be relied upon due to the lack of the Section 65B certificate. **IMEI records** (unique and recorded along with the phone number during a call) have been held to be proof of a **conclusive nature**.

In MOHD. ARIF @ ASHFAQ Vs STATE (NCT OF DELHI) 2023(3) SCC 654 para 22 the Hon'ble Supreme Court has held the evidence relating to electronic record, as noted herein before, being a special provision, the general law on secondary evidence under Section 63 read with Section 65 of the Evidence Act shall yield to the same. Generalia specialibus non derogant, special law will

always prevail over the general law. It appears, the court omitted to take note of Sections 59 and 65-A dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65-A and 65-B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this Court in **State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600**, does not lay down the correct legal position. It requires to be overruled and we do so. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65-B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65-B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.”

Smriti Madan Kansagra v. Perry Kansagra, 2021 (12) SCC 289.

21.6.The certificate under Section 65-B produced by Smriti merely states that the content of the emails placed on record were the same as the content of the emails on her inbox. This certificate does not certify the source of the messages allegedly received on the Blackberry of Perry, which were transferred to her cellphone. In the absence of a certificate in accordance with Section 65-B, with respect to the source of the messages, we cannot accept the same as being genuine or authentic.

Compact Disc's

The trial court day may not go off without receiving CDs. Receiving CDs and preserving them is one of the difficult tasks that trial courts face. Whenever a CD is produced before the court, it's always better to save it as an ISO image. In case of any damage, we can burn another CD which contains the same Hash value.

Kailas Baji Rao Pawar V/s State of Maharashtra AIR.2025 S.C 4294 (25-09-2025)

Illegal possession of contraband-Direction for retrial with judicial remand
 Challenge against , Being an electronic record, CD becomes an admissible piece of evidence once the requirement of Section 65B is fulfilled - Law does not provide that contents of video would become admissible only if reduced to a transcript in words of a witness who created video or was noticed in video - Author of video not only deposed that he had recorded a video, but also gave a certificate under S. 65B(4) of Evidence Act. Observation of High Court that video would become relevant only if it was played during deposition of each witness so that witness could explain its contents in his own words resulting in a transcript of video, was erroneous – Moreover video was only to corroborate oral testimonies regarding search and seizure operation - Even trial Court recorded that video was played in Court in presence of all accused, Counsels and Presiding Officer who could spot and confirm presence of witnesses as well as accused at time of search and seizure - Re-trial was not required only to understand video - Said reason assigned by High Court for ordering a re-trial was baseless. (Para No(s) 18, 19,20.)

K.K Velusamy vs N.Palanisamy 2011 (11) SCC 575 The Supreme Court held that a compact disc can be produced as a piece of evidence as per amended definition of ‘evidence’ in Section 3 and ‘electronic record’ in Section 2(t) of the Information Technology Act,2000 that includes a compact disc containing an electronic record of a conversation. The Court held that it is similar to a photograph and can be received in evidence under Section 8 of the Evidence Act, 1872. The tests indicated in **R.M Malkani vs. State of Maharastra (AIR 1973 SC 157)** for proving authenticity of recording, in addition to the requirements of Section 65-B would apply.

Bankers' Books Evidence

The definition of ‘Bankers’ books’ now includes books and records kept on microfilm, magnetic tape, or any other type of mechanical or electronic data gathering device. An entry in a bankers’ book in the electronic form may be

validated by means of a printout in accordance with **Section 2A of the Bankers' Books Evidence Act, 1891**. The printout must be accompanied by a **certificate of validation** by the principal accountant or branch manager, who must detail the computer system used and its safeguards.

XI. Authenticity, Characteristics, and Challenges of Electronic Evidence

Trustworthiness and Authenticity

The "standard of proof" in the form of electronic evidence should be "**more accurate and stringent**" compared to other documentary evidence. Trustworthiness has two dimensions: **reliability** (the record is capable of standing for the facts to which it attests) and **authenticity** (the record is what it claims to be). Authenticity is a condition precedent to admissibility. The mere possibility of tampering is not a sufficient ground to ignore electronic evidence; it must be weighed against all odds.

Components Subject to Authenticity Issues

Issues of authenticity may arise concerning:

- **The medium** (storage medium).
- **Content** (the message assembled from pointers to data).
- **The physical form** (script, formatting, inserts, time-stamps, operating system).
- **Intellectual form** (information configuration, content articulation, and annotations like digital signature authentication or urgency markers).
- **Action** (the record of the act or action that gave rise to the record).
- **People** (agents who create the content; author and addressee).

- **The archival bond** (ensuring the link is created and maintained when data is archived to prove the original data has not been altered).

Challenges to Authenticity in Court

Challenges to the authenticity of electronic evidence can include:

- Claims that records were **altered, manipulated, or damaged** between creation and court appearance.
- Questioning the reliability of the program that generated the record.
- Disputing the identity of the author (e.g., writer of an email or SMS).
- Failing to prove the message was directed to a particular person, especially where others might have access to the device.
- Questioning whether the person alleged to have used their PIN, password, or clicked 'I accept' actually carried out the action.

Fundamental Characteristics and Technical Challenges

1. **Dependency on Machinery and Software:** Electronic data is dependent on hardware and software (an interpreter) to be rendered into a human-readable format. An electronic document is better understood as a **process** (software) that recreates data every time a user opens it, rather than a fixed object.
2. **Mediation of Technology:** Data must be rendered through technology, meaning the same source object can be displayed differently depending on the screen or browser. There is **no concept of a single, definitive representation** of a digital object, which can lead to legal repercussions (e.g., unreadable formatting in contracts).

3. **Speed of Change (Technical Obsolescence):** Rapid changes in operating systems, application software, and hardware mean digital data may become **unreadable or unusable** due to a lack of backward compatibility. Technical obsolescence is a major problem.
4. **Volume and Replication:** Electronic documents are easy to copy, alter, update, or delete. Email and instant messaging are **duplicate and distributed technology**, allowing numerous copies to be rapidly distributed across geographical boundaries.
5. **Metadata:** Metadata is "data about data". All documents in electronic format contain metadata (explicit and implicit), and an electronic document **has to have metadata** to help interpret its purpose.
6. **Storage Media:** Electronic storage media is **inherently unstable and fragile**. If not stored correctly, it can deteriorate quickly without showing external signs.

XII. Modifications to the Indian Penal Code (IPC) (1860)

After the passage of the IT Act of 2000, numerous sections of the Indian Penal Code, 1860, were modified or added. These modifications dealt with the production of documents, summons, and fabrication of evidence, false entry, and false statement, including electronic records:

- **Section 172:** Evading the serving of a summons or other process by fleeing.
- **Section 173:** Intentionally blocking publication or serving of a summons or other process.
- **Section 175:** Intentional failure of a person legally required to deliver a document or **electronic record** to a public servant.

- **Section 192:** Fake proof that has been created.
- **Section 193:** Punishment for providing false evidence or creating it.
- **Section 204: Destruction with intent to prevent production as evidence** of a paper or **electronic record**.
- **Section 463:** Falsification of evidence and documents.
- **Section 465:** The cost of forgery.

XIII. Conclusion

The evolution of computer technology, pioneered by Charles Babbage, has made electronic devices an **indispensable part of human life**, necessitating the enactments of the **Information Technology (IT) Act in 2000** and the **Digital Personal Data Protection (DPDP) Act 2023**. Nonetheless, there are critical challenge, despite the widespread use of these devices, society remains **illiterate regarding the maintenance and management of electronic devices and evidence**. This lack of knowledge is compounded by the inherent risk that electronic records are **easy to manipulate and vulnerable to tampering**. We may fail if we ignore **AI**, which is a **medicine** as well as poison, we are doing injustice to the topic we are pondering today. While using the **AI**, please keep one thing in mind that it needs verification of the said **DATA**. Because it won't assure any accuracy, because it is a "కూపస్థ మండూకం", it will produce information from the data fed into it. The accuracy depends on the data fed into it. Therefore, the Artificial Intelligence created by the **Human God** has its own shortcomings. **If you feed accurate data, it will give an accurate Answer; if you feed fake data, it will give a fake answer..**

Consequently, the legal system, spurred by necessities like the recent pandemic, has developed a **more accurate and stringent** standard of proof for

electronic evidence. The most crucial legal trend is the mandatory nature of admissibility rules:

1. **Special Law Governance:** The general law on secondary evidence is superseded by the special provisions governing electronic records (IEA Sections 65-A and 65-B).
2. **Mandatory Certification:** The certificate required under **Section 65-B(4)** is a **condition precedent** to the admissibility of secondary electronic evidence. Recent rulings (up to 2025) affirm that the failure to produce this certificate **renders electronic records inadmissible**.

The integrity of this evidence depends heavily on meticulous handling and forensic expertise. Because digital data is highly volatile, collection requires strict adherence to procedures, such as preserving the original state of the device, using forensic drive imaging, and verifying the authenticity and integrity of copies using **cryptographic hash values**. Any lapse in the **Chain of Custody (CoC)** nullifies the legal value of the evidence.

Ultimately, the provisions introduced in the Bharatiya Sakshya Adhiniyam (BSA) which acknowledge electronic and digital records cannot be denied admissibility, expand the scope of **primary evidence to include temporary files**, and detail presumptions regarding secure signatures and electronic records demonstrate the legal system's decisive movement toward managing this complex form of proof. While new inventions are intended to make human life easier, citizens must use them with proper care, ensuring that a balance is struck in the application of these new technologies.