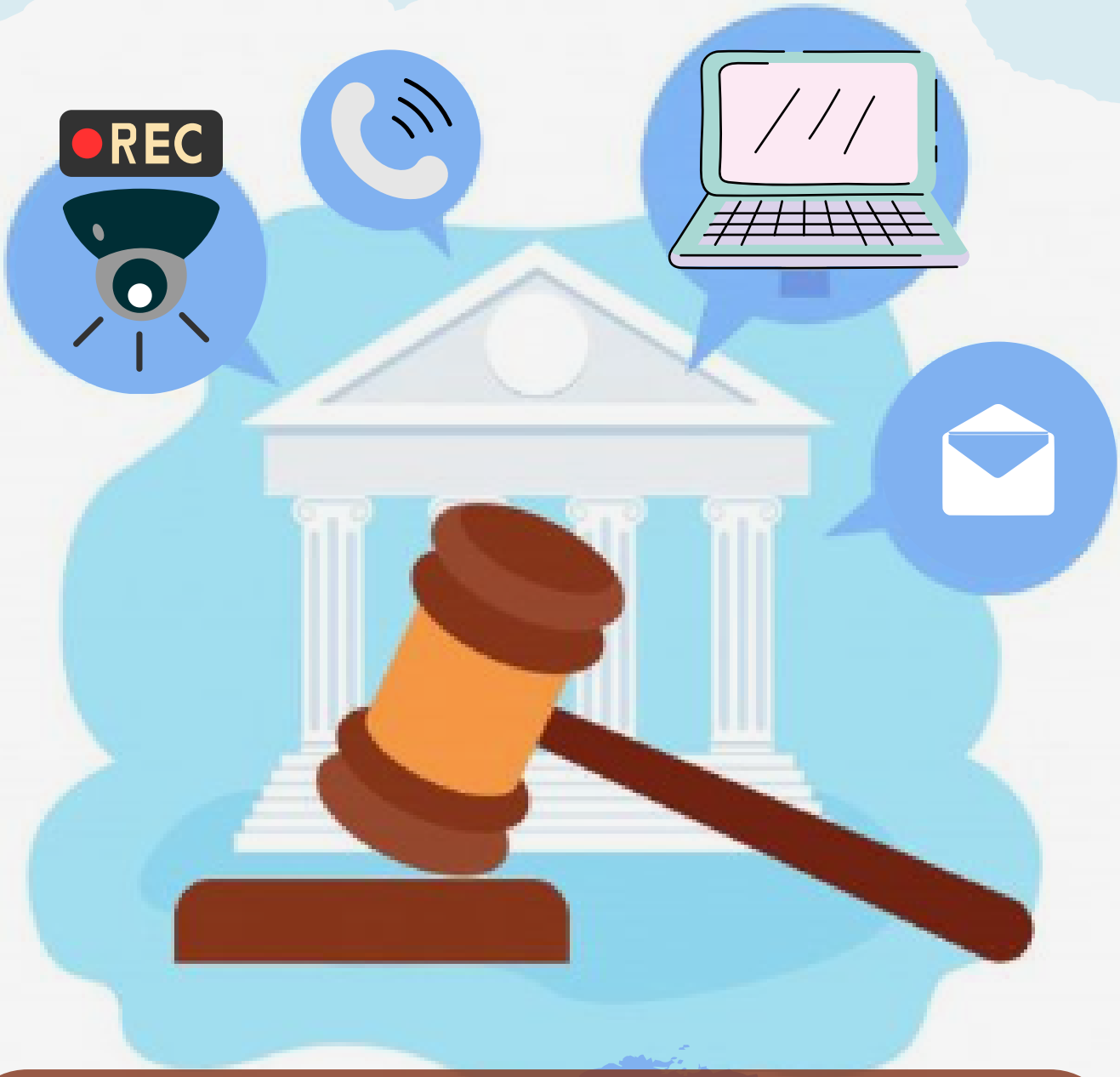

DIGITAL TRACES AS LITIGATION ACES

Wednesday Wisdom

07-08-2024

What is Digital Evidence?[1]

Digital Evidence is any information stored electronically that can be used as proof in a legal proceeding. It encompasses a vast range of data, from emails and text messages to financial records and social media posts. Give a thought to the three situations mentioned below before we move on to finding answers on Digital Evidence.

Imagine signing a property lease agreement digitally, avoiding the hassle of paperwork and in-person visits. A quick DocuSign can seal the deal efficiently.

WhatsApp screenshot of a payment confirmation can become vital evidence in a business dispute.

Imagine a public dispute escalating online, with both parties making damaging claims. Could these posts be used as evidence in court?

[1] The article reflects general work of the authors and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.

A New Era governed by Bharatiya Sakshya Adhiniyam 2023

The Indian Evidence Act, a century-old framework, has been superseded by the Bharatiya Sakshya Adhiniyam 2023. This landmark legislation, effective from July 1, 2024[2], introduces a modern approach to evidence, particularly digital evidence. A cornerstone of this Act is Section 61, which explicitly recognizes the admissibility of electronic records, dispelling the notion that digital format can be a barrier to acceptance of evidence.

RECOGNIZING AND ADMITTING 'ELECTRONIC RECORDS'

Indian Evidence Act, 1872 (IEA)

Section 65A establishes general admissibility of electronic records, treating them as documents. However, Section 65B imposes specific conditions, including a certificate from a responsible official, for electronic evidence to be accepted.

Bharatiya Sakshya Adhiniyam, 2023 (BSA)

Section 63 governs electronic evidence admissibility, mirroring IEA's provisions and specifically mandating a certificate to be issued by an expert to enable a digital document to be considered as digital evidence.[3] Section 39(2) of BSA mandates that an expert, known as an Examiner of Electronic Evidence (as per the Information Technology Act, 2000 ("IT Act")), must provide an opinion when a court needs to analyze digital information. Section 79A of IT Act empowers the Central Government to specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. The IT Act introduces a standardized certificate format, with distinct sections for the presenting party and an expert.

[2] https://timesofindia.indiatimes.com/india/three-new-criminal-laws-coming-into-force-across-india-on-july-1-what-it-means/articleshow/111385520.cms

[3] Page 46-47 of BSA, 2023 https://www.mha.gov.in/sites/default/files/250882_english_01042024.pdf

ADMISSIBILITY OF E-EVIDENCE

Indian Evidence Act, 1872 (IEA)

Section 65B(1) states that any information contained in an electronic record, stored, recorded, or copied as a computer output, is considered a 'document' and is admissible as evidence without needing further proof or the production of the originals.

Bharatiya Sakshya Adhiniyam, 2023 (BSA)

The BSA expands the definition of 'document' to include electronic and digital records. Section 61 unequivocally permits their admissibility, subject to authentication requirements mentioned under Section 63.

A new illustration is also added to expand electronic record meaning to state “An electronic record on emails, server logs, documents on computers, laptop, or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents.”

AUTHENTICATION OF E-EVIDENCE

Indian Evidence Act, 1872 (IEA)

Section 65B outlines conditions for admitting electronic evidence, including regular computer use, data input, and operation. A certificate from a responsible official is mandatory.

Bharatiya Sakshya Adhiniyam, 2023 (BSA)

Section 61 grants equal legal status to electronic and digital records. While adopting a similar certification process as the IEA, the BSA incorporates stricter safeguards to address cybersecurity challenges.

Embracing Digital Transformation

The Indian judiciary is undergoing a digital transformation. From the virtual courtroom to online case management, the legal landscape is rapidly evolving:

- **Virtual Hearings**
  - Remote proceedings through video conferencing have become the norm, enhancing accessibility and efficiency.
- **Online Filing**
  - Digital submission of legal documents has streamlined processes and reduced paperwork.
- **Digital Case Management**
  - Online case tracking andmangement systems are improving case handling and transperancy.

Building strong Digital Evidence:

Imagine a fintech organisation booming with digital transactions. Every online payment, customer interaction, and internal communication generates a digital trail. This digital footprint can be a double-edged sword. To ensure it's a shield and, not a liability, understanding how to create and preserve digital evidence is paramount. Following are the Dos and Don'ts of building a rock-solid digital case:

✓ DO'S

Robust Backup Systems: Protect digital data from loss or alteration by implementing robust backup systems and access controls.
er stop innovating

Chain of Custody: Maintain a detailed record of who accessed, handled, or modified digital evidence.

Authenticity: Verify the integrity and origin of digital files to establish their authenticity.

Data Experts: Consider involving data experts to extract and analyse data effectively.

✗ DON'TS

Alter or Delete: Avoid modifying or deleting digital information as it can compromise its integrity.

Delay Preservation: Act promptly to preserve digital evidence to prevent loss.

Ignore Metadata: Metadata contains valuable information about a file, so don't overlook it.

Overlook Cloud Storage: If using cloud services, understand the provider's data retention policies.

Neglect Employee Training: Educate employees about the importance of digital evidence and proper handling.

Deepfakes, highly realistic synthetic media, pose a significant challenge to the admissibility of digital evidence. Their ability to convincingly mimic individuals or manipulate content undermines the authenticity and reliability of digital information. Robust forensic techniques are crucial to detect these forgeries and ensure the integrity of digital evidence in legal proceedings.

In the case State of Karnataka v. T. Naseer @ Thadiantavida Naseer (November 8, 2023) [4] which revolved around the trial of the serial bomb blasts which took place in Bangalore on 25.07.2008. The prosecution wanted to rely on certain electronic evidence such as one Laptop, one external Hard Disc, 3 Pen Drives, 5 floppies, 13 CDs, 6 SIM cards, 3 mobile phones, one memory card and 2 digital cameras etc. which were seized at the instance of an accused. The original electronic devices were submitted before the Trial Court along with the additional chargesheet dated 09.06.2010. However, the certificate required under the IEA was submitted in 2017. The lower courts had rejected the prosecution's attempt to introduce a certificate under Section 65B of the Indian Evidence Act, crucial for authenticating electronic evidence, at a later stage of the trial. The Supreme Court intervened and emphasized that the object of the Code is to arrive at truth. The Apex Court concurred with the earlier judgements and laid down that, “So long as the hearing in a trial is not yet over, the requisite certificate can be directed to be produced by the learned Judge at any stage, so that information contained in electronic record form can then be admitted and relied upon in evidence.”

Thus, the electronic evidence was taken on record and the lower court's decision was overturned. The Apex Court emphasized the importance of fair trial for both parties and allowed the introduction of the certificate, setting a precedent for the admissibility of digital evidence even at later stages of a trial.

[4] The State Of Karnataka vs T Naseer @ Nasir @ Thandiantavida Naseer 6th November, 2023 INSC 988

Conclusion:

The BSA 2023 ensures that digital evidence is admissible provided it is authenticated properly, thus enhancing the credibility of judicial proceedings. This legislation is a critical step in the legal digital transformation India is undergoing, aligning the country's legal processes with global technological advancement. This forward-thinking legislation not only ensures justice but also positions India at the forefront of global legal tech.

For any feedback or response on this article, the authors can be reached on atharva.amdekar@ynzgroup.co.in and Gauri.Joshi@ynzgroup.co.in

Author: Atharva Amdekar

Atharva is an associate at YNZ Legal.
By qualification he is Bachelor of commerce and Bachelor of Law from Mumbai University

Co-author: Gauri Joshi

GAURI is an Associate at YNZ Legal. By Qualification she is Bachelor of Commerce from Mumbai University and Bachelor Of Law from SNDT University.