



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

YOUR DIGITAL FOOTPRINTS IN COURT: HOW SOCIAL MEDIA EVIDENCE IS CHANGING CRIMINAL TRIAL

- *Sarisha*

ABSTRACT: Social media has become a routine source of evidence in Indian criminal trials. With the increased use of such platforms, being used for committing crime, a series of questions related to privacy, freedom of speech, admissibility, and reliability arises when digital footprints from such platforms reach the courtrooms as evidence. This blog will delve into admissibility of such evidence which runs through a strict statutory filter, first under Section 65B of the Indian Evidence Act and now Section 63 of the Bharatiya Sakshya Adhiniyam.

INTRODUCTION

Can a string of Instagram messages decide whether someone walks out of a courtroom an acquitted man or a convicted one? Increasingly, in Indian trial courts, the answer is yes.

Social media platforms such as Facebook, WhatsApp, Instagram, LinkedIn and X (formerly Twitter) have become sources of digital evidence in modern legal proceedings. Evidence from these platforms' spans over messages, posts, comments, photos, videos, and other digital activities such as likes and shares.

In both civil and criminal cases, social media evidence can help establish motive, intentions, relationships, and timelines. It is increasingly used in matters involving defamation, cyber harassment, fraud, conspiracy, and other criminal offences.

FROM IEA 1872 TO BSA 2023

The Indian Evidence Act of 1872 recognized electronic/digital records through Section 65B¹, which governed the admissibility of electronic evidence. However, those provisions were

¹ Indian Evidence Act, No. 1 of 1872, § 65B (India).

introduced in 2000 and did not cover many modern forms of digital communication that are more complex and often unclear. The Bharatiya Sakshya Adhiniyam of 2023 (BSA) broadened the scope and interpretation of digital evidence. Unlike the Indian Evidence Act, which addressed electronic records through specific clauses, the BSA blends them directly into its basic definitions. The definition of "evidence" now includes information given electronically as oral evidence and digital records as documentary evidence. The BSA further updated the legal framework in Section 57², which relates to primary evidence. It recognizes that digital information often exists in various forms and locations. For instance, copies of the same electronic record can be stored across different files, devices, servers, or temporary storage areas and can be considered as primary evidence. Similarly, video recordings that are stored and transmitted at the same time are regarded as primary evidence. Another important change is found in Section 61, which treats electronic and digital records the same as traditional documents.³ Courts cannot reject evidence simply because it is in digital format, as long as the statutory requirements are met. Section 63⁴ further expands the kinds of acceptable electronic evidence to include records stored in semiconductor memory, smartphones, and other communication devices. It also keeps the certification requirement, similar to the previous Section 65B of the Indian Evidence Act, but with better safeguards. Parties must now submit a specific certificate that includes a section filled out by the party and another verified by an expert to confirm the authenticity of the digital record.

THE SECTION 63 CERTIFICATE AND JUDICIAL INTERPRETATIONS

In *Anvar P.V. v. P.K. Basheer* case ⁵, the Supreme Court held that the certificate is mandatory, with no exceptions. A few years on, *Shafhi Mohammad v. State of Himachal Pradesh* tried to soften that position for a party who never had control over the device that produced the record ⁶. High Courts split between the two views, and trial lawyers were left guessing which one their bench would follow. The question was finally closed in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* ⁷. A three-judge bench reaffirmed *Anvar* and held that the certificate is mandatory unless the original device itself is produced in court.

² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 57 (India).

³ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61 (India).

⁴ The Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India).

⁵ *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

⁶ *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

⁷ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).

Getting the certificate right is only the first hurdle. Social media evidence raises a second, harder question: what does a message actually prove? A 2023 study of more than three thousand sexual assault forensic examination records in the United States found that cases beginning on dating apps were significantly more violent than other acquaintance assaults, and that chat logs alone rarely settled the question of consent, since consent given for one part of an interaction does not extend to the rest of it.⁸ For example, a person may have agreed in messages to meet someone or engage in certain activities, but that does not mean they consented to everything that happened afterward. Consent can be limited, conditional, or withdrawn at any stage. Courts reading such chats should check the timing and conduct around the message, not just the words on the screen, and no certificate under Section 63 does that work for them in such cases.

There is a constitutional layer sitting underneath all of this, which poses another hurdle. The Supreme Court in the case *K.S. Puttaswamy v. Union of India*⁹ recognized privacy as part of Article 21, hence, putting a person's social media history into a chargesheet stopped being a purely procedural act and became a question of proportionality. They need a reason that the intrusion of a person's privacy fits the offence under investigation, rather than a search through years of someone's digital footprints just because the data happens to be there.

None of this makes social media evidence unreliable. It makes it powerful and fragile at the same time. Powerful, because platforms timestamp almost everything and rarely let data disappear completely, which forms the digital footprints. Fragile, because the change in jurisdiction hampers the case easily when the evidence sits on a server abroad, governed by a company's own policy and its own timeline for responding to an Indian court.

CONCLUSION

Digital evidence has transformed the way facts are presented in the courtrooms. BSA 2023 has expanded the scope of digital evidence and strengthen its legal framework. A screenshot of the WhatsApp chat rarely tells the full story. The court needs to put emphasis on privacy, context, facts, actions, and intentions. Balancing proportionality with admissibility of digital evidence.

⁸ Julie L. Valentine, Leslie W. Miles, Kristen Mella Hamblin & Aubrey Worthen Gibbons, *Dating App Facilitated Sexual Assault: A Retrospective Review of Sexual Assault Medical Forensic Examination Charts*, 38 J. Interpers. Violence 6298, 6298–6322 (2023).

⁹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).