Page 498 - 506 **DOI:** *https://doij.org/10.10000/IJLMH.11532*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Social Media as a Source of Evidence

SARVESH RAIZADA[1]

ABSTRACT

The current research focuses on the control of a communication medium that has ushered in a new age of communication pace. With the advent of social media, the internet, which has impacted many aspects, has revolutionized the information age. In certain respects, the emergence of the internet was unlike the emergence of any other set of creative communications technology. It introduced new features that not only shattered a slew of barriers between personal and mass communication, but also reversed a centuries-old mass media paradigm. The new communications movement has empowered content consumers to become content creators themselves. User produced content has grown from humble beginnings, such as the opportunity to post text or photographs on personal web sites, to an extraordinary global influx of mixed original and reused content that exists in a variety of ways and formats. This today include video sharing, social networking, blogging, and tweeting, among other things. It's been dubbed "social media" as a whole. When opposed to other types of advertising, social media has its own set of characteristics. This paper focuses on how social media influences or facilitates the procuring of evidence in the judicial system. Because of its pace and reach, once material is released, it is instantly accessible to a possible global audience. Social media is used by people of all ages and professions. Not just is social media altering the way we interact.

Keywords: *Media as Evidence, Social Media in Indian Courts, Authenticity of Evidence.*

I. INTRODUCTION

For the next decade, technological development is the path ahead. In today's fast-paced world, every person uses social media sites such as WhatsApp, YouTube, Instagram, or Facebook; some of these uses are positive, while others are negative. Social media can be described as collaborative computer-mediated technologies that facilitate the production and sharing of ideas, knowledge, thoughts, career preferences, and other forms of speech through virtual communities and social networking websites. With the advancement in technology, there has been a rise in crime rates and offences committed using technology. Cybercrime is a common term for this kind of crime. Cybercrime was not always known or thought to exist, but it is now

[1] Author is a student at Alliance University, Bangalore, India.

 [ISSN 2581-5369]

being investigated as a field of study and expertise. Communication must be brought before the victim in order to be charged with cybercrime, nor can communication that occurs through this means which is posted on a social media site be used as evidence in a court of law? Can social media posts be considered admissible testimony, despite the fact that many people doubt their accuracy? However, e-communication would not have to be brought before a judge to confirm the evidence of a crime of cybercrime.

E-communication, such as comments and tweets, is often required in court to show the seriousness of certain offences, such as defamation. When we receive anything as simple as a wedding invitation from social media, the seriousness of social media data is amply demonstrated. In India, investigative services, also known as intelligence agencies and police forces, have recently begun generating messages shared on Twitter, Facebook, and other social media sites by individuals. They do so in accordance with the Indian Evidence Act. Union Home Minister Rajnath Singh recently admitted during a press conference in 2016 that the government has established a playbook on social media policy against the IS for the purpose of successful surveillance of the undiscovered side of the internet, such as the Dark Web. Cyberspace refers to any kind of connectivity that aims to link the world through networks and mobile devices. When we think about social media these days, we think of platforms like Facebook, Twitter, Instagram, Snapchat, WhatsApp, among others. Any of you cannot even recall a time before social media, which is both amusing and hilarious. It's also impossible to picture a future without social media, to be honest. These social networking platforms have evolved into more than just places to post your favourite selfies and memes; they have also evolved into a powerful tool. When used correctly, a tool will draw people together, give power to the voiceless, and bring down corrupt dictatorships, such as the one we saw in Egypt in 2011, when hundreds of thousands of protesters assembled in Tahrir Square.

A coin, though, still has two sides. People often use social media for cyberbullying, sharing false information, trolling, catfishing, and violating privacy. Terrorist organisations, on the other hand, use social media in the most dangerous and bloodcurdling ways. Al-Qaeda is one of these organizations that makes heavy use of social media. ISIS, or the Islamic State in Iraq and Syria, is another organization that uses social media to harass the public by uploading images of beheadings. Every day, Facebook users upload over 1.5 million pieces of content (web links, news articles, blog entries, comments, photographs, and so on). Social media has surpassed pornography as the most popular online operation.

 [ISSN 2581-5369]

II. ADMISSIBILITY OF ELECTRONIC EVIDENCE IN THE INDIAN COURTS

The Indian Evidence Act has been revised, specifically to allow electronic evidence (record) accompanied by paper-based records to be used as evidence in Indian courts. Granting the status of archives for the purpose of adducing testimony to electronic databases is one of the most significant amendments. Furthermore, the concept of 'admission' was revised and modified to include information in electronic form, implying that any contact with any fact in question or any other related fact is prohibited. Section 22A, on the other hand, was inserted to ensure that oral testimony was relevant. Oral admissions as to the contents of electronic records are not necessary until the authenticity of the electronic records created is in doubt.

The incorporation of Sections 65A and 65B under the second schedule of the Information Technology Act is arguably one of the most significant amendments to the Evidence Act. This establishes a distinct and unique method for adducing testimony in cases involving electronic documents. According to Section 65B, any material found in an electronic archive is considered a text and is admissible in testimony without further proof of the original's creation. It also establishes requirements for the admissibility of proof, all of which must be met. They are as follows:

1. The computer output containing the relevant information was derived from a computer that was used regularly to store and/or process information for the purpose of any activities that were regularly carried out during the era by the individual legally controlling the use of the machine at the time the electronic record was created. In the normal course of business, the sort of information stored in the electronic record was fed into the machine on a routine basis.
2. The material found in paper archives is a duplicate of the original printed document.
3. The material found in paper archives is a duplicate of the original printed document.
4. The machine was running correctly or, if not, was out of service for a period of time during the material portion of the period, but not to the extent that it affected the electronic record.

III. EVIDENTIARY VALUE OF SOCIAL MEDIA

The evidentiary importance of social media messages is explained by Criminal Procedure Jurisprudence. Certainly, there are benefits and sound policy arguments for accessing social media information involved in court proceedings; for example, images can be posted easily and shared within seconds, alerting police of offences in progress or those already committed. When it comes to the admissibility of social media data, it's just about getting the facts in a

 [ISSN 2581-5369]

legal way. More frequently than not, a lawyer prosecuting a lawsuit would need to view the public parts of a person's social media site to see if any of their accounts provide information pertinent to the case. According to Common Law, when undertaking an audit pursuant to a lawsuit, one must consider the relevant code of ethics. For example, bypassing settings or adding someone as a friend in order to obtain access to private or non-public areas of the subject's account is immoral and improper. Furthermore, this type of behaviour on social media can render social media evidence inadmissible in court. In India, we've had a special division of cyberspace crime investigation since 2000, as well as a separate law called the Information Technology Act, 2000. Other supplemental cyber laws are used to deal with those offenses in their place. These cases are only called to the attention of a special court. The screening procedure for the admissibility of all online documents, tweets, and posts remains the same as described in Section 22A of the Indian Evidence Act.

In certain cases, like violent offences like kidnapping, such testimony is also presented in the Magistrate's Court, where it must be justified when there is a pending lawsuit. "Party's parole admissions receivable to prove the contents of a paper without warning to prove or without according to the absence of original," according to English statute. However, under Indian law, this is not permissible or relevant.[2]

IV. AUTHENTICITY OF SUCH EVIDENCE

In India, law enforcement detects a criminal and then requests evidence from platforms. To demand the publication of an account's contents, WhatsApp, for example, includes a Mutual Legal Assistance Treaty order or a letter rogatory. WhatsApp will take care to keep account records for 90 days awaiting receipt of formal legal process in connection with official criminal investigations. The WhatsApp Law Enforcement Online Request System can also be used to file formal preservation requests quickly.

A law enforcement officer can use the WhatsApp Law Enforcement Online Request System to respond to a matter involving imminent harm to a child or a risk of death or serious physical injury to any person that requires immediate disclosure of details. Non-law enforcement agents' demands for information are categorically denied by WhatsApp. WhatsApp does not keep data for law enforcement purposes until they get a legitimate retention request until a customer deletes the content from their site. Since WhatsApp does not store messages or transaction records of those messages after they have been delivered. Undelivered texts, according to them,

[2] Tejas Karia et al,*The Supreme Court of India re-defines admissibility of electronic evidence in India*,Digital Evidence and Electronic Signature Law Review, 12 (2015).

 [ISSN 2581-5369]

are erased from their servers after 30 days.

The accuracy of an electronic document determines its evidentiary significance. The Indian Evidence Act, 1872, has provisions for dealing with the evidentiary importance of electronic documents. The Indian Evidence Act discusses the validity and admissibility of photographic evidence in the form of an electronic archive, as well as its requirements, which are comparable to those of traditional records. Under sections 65A and 65B of the Evidence Act of 1872, the evidentiary validity of electronic documents is generally debated. The requirements and process for proving an electronic document in a court of law are laid out in Section 65-B of the Indian Evidence Act. Section 65B is important because it understands that the original primary testimony in electronic documents is unlikely to be taken before the court, and even though it is, the evidence will be in binary form, which the court will not be able to understand. The net result of Section 65B is that the computer's output, whether in the form of a printout or data copied on CD/DVD, is admissible in court if those requirements are met. This is what Section 65B is all about (1). To be admissible in a court of law, the output of an electronic document must be filed with a certificate u/s 65B (4) of the Evidence Act. An individual in a responsible role with respect to the machine on which the data is generated must grant such a certificate. The credential must certify the requirements set out in S. 65B(2), which include the accuracy of records and computer systems, the manner in which the performance of an electronic record is produced, the identity of the device used, and the specifics of the device used, including the original device. The certificate's entire purpose is to ensure, once again, the source's credibility and data's accuracy, so that the court can put confidence in it.

Lawyers who present social media information in court should be willing to "over-authenticate" their evidence by laying a basis that, if possible, excludes the risk that the material was made by an imposter. The proponent's job should be completed if a witness can confess to writing a post or owning a social media page and will lay a basis to justify the admission. However, the Fifth Amendment can prevent this form of testimony in criminal trials (and even certain civil cases) if the witness feels that giving such testimony may lead to self-incrimination. If a witness feels that giving such evidence may lead to self-incrimination, he or she can refuse to give it. Regardless, hostile witnesses are often unable to agree that they made a post or that they recall doing so. Authentication of social media data should also be based on foundational testimony regarding three topics:

- Circumstantial evidence of authorship or account formation
- How the evidence was discovered and validated (i.e., "chain of custody")

 [ISSN 2581-5369]

- How the social media site itself gives indicia of authenticity to the evidence.

V. LOOPHOLES IN USING MEDIA AS A SOURCE OF EVIDENCE

The digitalization of our country and the exponential development of technologies are the primary drivers of proof recording and legal reforms. The method of recording electronic documentation poses not only ethical concerns, but also social concerns. For most of us, our mobile phone holds a wealth of knowledge about many facets of our lives, and social media is the place where people express their feelings and meaningless everyday activities. In recent years, the media has placed a greater emphasis on the collection of electronic data. The use of knowledge derived by social media and networks is the most relevant subject on which the media is attempting to rely further. As a result, current issues and potential concerns of electronic proof must be discussed. It is necessary to establish a regulatory structure, to address various legal issues in various jurisdictions, and to consider potential challenges. The below are the major concerns:

- The use of e-discovery and e-disclosure to gather and produce facts in court
- The validity, admissibility, and trustworthiness of electronic proof submitted in court.
- The use of social media and emoji's in the presentation and application of visual information submitted in a court of law.

(A) The accuracy of digital documents can be challenged in a number of ways:

- Who Is the Author of the Records, an Identity Management Challenge? The author of the digital material offered into testimony is sought in a variety of forms by courts. It is critical for the proponent to provide testimony on who the author is, whether the letter, text, film, or photo was posted on a website.
- Is the computer program that created the various documents trustworthy? Was the computer's performance as accurate as it should have been?
- Were the documents tampered with, corrupted, or destroyed after they were made? Photographs and images can be altered using various Photoshop websites and graphic design applications, while hackers can modify websites, databases, and other electronic media. They usually hide their trails by altering audit log data.

(B) Information on social media sites.

Due to the obvious endless number of people who use social media sites like Facebook, Myspace, and LinkedIn, content has been generated that is beyond the reach of any one individual or organisation. In addition, courts typically extend a higher requirement to the

authentication of information from social networking networks where there are no restrictions on who can build a profile. Courts cannot always assign a single post to the person who owns the site since anybody can build a social network profile anonymously. It's tough to figure out who wrote the post because it can be done on a public machine, such as one in a library or a hotel.

(C) Blurred the difference between Primary and Secondary Evidence

By incorporating all types of computer proof in the scope of primary evidence, the act effectively blurs the line between primary and secondary forms of evidence. Since the data derived by computer-generated records is complex and cannot be readily produced in physical form, an allowance has been made for it. As a result, it would be a good case to argue that if the word document is the original, then a printout of the same can be viewed as secondary evidence. However, it can be noted that creating a word document in court without the use of printouts or CDs is almost impossible.

(D) Unjustly Prejudiced

The term prejudicial refers to a tendency to persuade based on historical experiences rather than real facts of the situation at hand. Proof that is detrimental, injurious, or skewed in favor of the case without establishing any valid facts or enraging the judge without presenting some material facts is often exempt from court proceedings. A child's photograph, for example, wrapped around the victim's neck.

(E) Wastes time

At court cases, attorneys defending their clients often offer testimony or witnesses that may waste the Court's time; however, those witnesses or evidences are usually omitted from the proceedings. For e.g., it is a waste of time for the Court where the advocate would produce twenty different individuals to show that the accused is a trustworthy individual.

(F) Misleading

If the testimony shown is diverting the jury's or judge's interest away from the core topic or substance of the prosecution, it is called false evidence and should be removed from the trial. In a case of rape, for example, a minor's gender is meaningless since the key truth to ascertain is whether or not the minor was raped, because it is unimportant to know which gender the minor was.

(G) Hearsay evidence

When an individual is not directly present but has knowledge of an incident from someone else,

 [ISSN 2581-5369]

this is known as hearsay testimony. Such testimony is inadmissible in court and everyone would fault the other one for rescuing the accused or allowing them to avoid prosecution. For example, if witness "A" says that another witness "B" said the defendant hit the victim with a stick, then the prosecution tries to use the evidence to prove the defendant hit the victim, it is called hearsay.

(H) Character

The proof provided by the appellant party to show the defendant's character has some characteristics that are omitted from the court proceedings until the defendant presents the character evidence first in the hearing.

(I) Expert Testimony

Expert testimony can only be used in court if it was submitted by an expert rather than a layperson. The testimony of a layperson is not admissible in trials.

(J) Privileges

The Court would not admit any documents received under the attorney-client privilege, as well as any other self-incriminating information. Such evidence is classified in nature and will cause the attorney to perjure himself, making it inadmissible in court.

VI. INTERNATIONAL CASES

In ***Romano v. Steelcase Inc***.[3]. (a September 2010 New York personal injury case), the Court dutifully allowed the defendants access to the plaintiff's "existing and past Facebook and Myspace profiles, as well as websites, including pages that have been removed and have important material, even if the information was not originally publicly accessible." This was permitted because her Facebook profile showed her posing peacefully in a photograph taken outside her home, despite the fact that she said she had been injured and was confined to her bed. The Court then decided to allow the complainant to use the self-set privacy controls on a website as a defence. The key goal is to enable people to share more on how they live their social lives. As a result, the opposing side could be denied access to information that may be useful in ensuring a fair trial. The court reasoned that protection is not an exception, regardless of the privacy settings used.

Zimmerman v. Wels Market Inc.[4], a personal injury lawsuit, is another significant case involving the admissibility of social media content in court. Based on the public knowledge

[3] Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (2010).
[4] Zimmerman v. Weis Markets, Inc., PICS Case No. 11-0932 (2011).

shown on the plaintiff's Facebook profile, it was understood that there was material that was personally held content that was pertinent to the lawsuit. The plaintiff's Facebook profile listed his hobbies as "riding" and "bike tricks," as well as recent photos of the plaintiff with a black eye and his motorcycle after a crash. The Court then decided in favour of the defendants, granting them permission to conduct discovery and granting them access to the plaintiff's non-public portions of his Facebook profile as well as his Myspace site. This was done in order to disprove claims of lasting harm to the plaintiff's welfare and well-being.[5]

VII. CONCLUSION

The issue is that in arbitration, social media platforms are less than friendly. People who post on Facebook or other sites often do so themselves, so it's rare that this is the source of the issue. The issue is convincing the corporation to give you access to the customer details so you can confirm you're dealing with the right guy. Since Facebook is not an Indian organization, obtaining information from a Facebook representative is challenging.

When we consider the role a social media post can serve in a civil or criminal case, we can see how important it can be. As we saw above, social media postings have been used in the past to support an argument in court that would otherwise be impossible to assert. The challenge of social media evidence is ensuring that there is adequate evidence provided to justify and uphold the posting to be as it appears to be. The fundamental rule of admissibility of all evidence is its application to a particular case, and if this theory is applicable to a case involving social media, admissibility will no longer be an issue in a court of law.

*****

[5] Bradley v. State, 359 S.W.3d 912 (2012); Elonis v. United States, 192 L. Ed. 2d 1 (2015).

 [ISSN 2581-5369]