Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Scope of Admissibility of Electronic Records

Fardeen Haque[a]

[a]Amity University, Kolkata, India

Received 22 July 2022; *Accepted* 21 August 2022; *Published* 23 August 2022

The advent of the modern world has posed many challenges and one of them being the regulation of cyberspace and dispensing judgement for the infringement of rights regarding the digital extent. The collection of data and its transmission through electronic means such as mobile phones, computers, laptops, networks, etcetera in a malign sense come under cybercrime and the documented evidence gathered from such means is called electronic evidence. The authenticity and validity of digital evidence are always in the debate because of its highly temperable nature and also because it requires specialized institutions and experts to verify its accuracy. The paper deals with the basis on which admission of electronic evidence and other records are made possible and how such information is analyzed for serving justice under the Indian Evidence Act, IT Act, and the statutes on Cybercrime.

Keywords: *electronic evidence, cybercrime, evidence act, data, data transmission.*

INTRODUCTION

Even though electronic gadgets and their use started around the 17th Century but they were never a household product until the 21st Century. This century saw the biggest breakthroughs in science and technology which changed the way we communicate, connect, we engage with our environment. In today's world, we live in an environment of technology and media that is characterized by a wealth of information, rapid changes in technology tools, collaboration on

an unprecedented scale, and personal contributions. This has enabled humankind to be free of barriers and opened up a whole lot of opportunities in different fields ranging from business to administration, academics to recreation but has also surged an increase in unlawful activities. Therefore, there is a need to reform the information technology laws and admissibility rules of electronic evidence in both civil and criminal issues. This change was initiated by the United Nations Commission on International Trade Law (UNCITRAL), the core body of the United Nations responsible for developing model laws for electronic commerce. The Computers and Information Technology Act 2000 is a major law dealing with illegal activities in cyber-states and e-commerce and applies throughout India and outside India when criminal offences are committed on computer systems or networks established in India was done. The law amends the Indian Evidence Act of 1872 to include provisions on the permissibility of electronic evidence in court. While contents of a document can be proven by both primary and secondary evidence definitions which are stated in section 62 and section 63[1] respectively, the court withheld that as mentioned in section 64[2], proof of document be given only by primary evidence except in cases where the conditions provided in section 65[3] are fulfilled. The provisions amended under section 65, that is sections 65A and 65B[4], state that electronic records are deemed admissible in court only if followed by the conditions mentioned in 65B. Section 65B states that the information contained in an electronic document is acceptable as evidence and is considered original only if it meets the conditions set forth in Sections 65B (2) to 65B (5)[5]. Therefore, the electronic evidence must be accompanied by the certificate generated upon completion of the checklist provided in Section 65B.

ELECTRONIC EVIDENCE IN THE INDIAN EVIDENCE ACT

The modern world has been revolutionized with the technology of computers and digital devices which has allowed humankind to receive and send information, access, and store data at unimaginable speed and within the reach of a click. The dependence of man on electronics

[1] Indian Evidence Act, 1872, ss 62 and 63
[2] Indian Evidence Act, 1872, s 64
[3] Indian Evidence Act, 1872, s 65
[4] Indian Evidence Act, 1872, ss 65A and 65B
[5] Indian Evidence Act, 1872, s 65B(2) and (5)

and digital tools has subsequently increased the rates of cyber crimes and crimes operated through the use of computers and other electronic devices. The increase in this vice peddled through screens and often untraceable networks have always put new issues while serving justice. The lack of original sources and their very capricious nature raises many questions about the admissibility of electronic evidence in court. The Information Technology Act of 2000 created a new amendment to the Indian Evidence Act of 1872. This includes electronic evidence and its court activation provisions. The law arose from the need to implement a national e-commerce framework and create legislation to ensure legal approval of transactions conducted using electronic data interchange and other electronic communication means. The IT Act and its amendments are based on the United Nations Commission on International Trade Law ("UNCITRAL") Model Act on Electronic Commerce. Information law defines electronic records as data stored, received, or transmitted in electronic form, microfilm or computer microfiche (document for microfilm), recorded or generated data, images, or sound. The information which can be transmitted or stored in a digital manner and has probative value is called digital or electronic evidence. Digital evidence amasses all the sources and media, such as telecommunication devices, recording tools, e-mails, instant messaging histories, transactional logs, accounting databases, CCTV footages, etc., through which information of probative nature could be acquired, stored, or transmitted to and from and its veracity and relevance could be brought about in the course of a trial to support or denounce a fact in issue.

Evidence as per the Indian Evidence Act, 1872 mentioned in section 3[6], means and includes

- All the statements that the court permits or requires to be made before it by witnesses, in relation to the matters of fact under inquiry; such statements are called oral evidence
- Documentary evidence is any evidence, including electronic recordings, that is generated for a court's review. Additionally, "document" is defined in the same section as any information that is expressed or described on the material using letters, figures, markings, or a combination of those, and that is intended to be used or that may be

[6] Indian Evidence Act, 1872, s 3

used to record such information.[7]

Electronic records are considered documentary evidence and are considered as dependable evidence than oral evidence. Evidence may be given of facts in issue or any other facts which are declared relevant mentioned in various sections of Chapter II of the Indian Evidence Act. The phrases "contents of papers" were changed to "contents of documents or electronic records" in relation to the documentary evidence indicated in section 59[8], and sections 65A and 65B were added to improve the admissibility standard for electronic evidence. Without a document, oral testimony cannot adequately establish a document's authenticity or prove its contents since it would be impossible to compare the testimony to the absent document and it would also violate the hearsay rule (since the document is absent, the truth or accuracy of the oral evidence cannot be compared to the document). According to section 61[9] of the Indian Evidence Act, the contents of the document may only be shown via either primary or secondary evidence. Primary evidence states that a document is itself the primary evidence required to prove its content. Primary evidence has the faculty to prove the veracity of a document and its contents and is, therefore, a mandatory way of proving the contents of a document as mentioned in Section 64[10] of the Indian Evidence Act except for some cases where secondary evidence can also be considered for the proof of documents, the conditions of which are mentioned in Section 65. The Evidence Act defines secondary evidence as any copies of the original document held by any authority and with proper certification from the same, copies made according to the same mechanical processes that prove the accuracy to its original, copies made from or compared with the original, copies made by parties who did not execute them, and oral reports of the contents of the documents by someone who has personally observed the facts of the document. Section 65 maps out the criteria whereby the proof of documents can be proven by secondary evidence, which is as follows:

- when the original document is in possession of the party against whom it was to be

[7] Indian Evidence Act, 1872, s 2
[8] Indian Evidence Act, 1872, s 59
[9] Indian Evidence Act, 1872, s 61
[10] Indian Evidence Act, 1872, s 64

drawn, with a person of inaccessible circumstance, any person legally bound within section 66[11] yet they do not produce it.

- when the contents of the original documents have already been proven or admitted in writing by the person against whom it was to be proved.
- when the original document does not exist due to circumstances not arising from his own default or neglect.
- when the original document is of immovable nature.
- when the original document is a public document.
- when the original is any document whose certified copy is permitted by this act or any other jurisdiction within India.
- when the original document is a collection of many accounts and only the fact to be proved is the general result of the whole collection.

The special provision made under section 65 for the inclusion of the terms for the admissibility of electronic records as evidence points to the secondary nature of such records. Section 65A, included after the authorization of the Information Technology Act, 2000, states that the contents of the electronic records may be proved in accordance with the provisions of section 65B. The Supreme Court's three-judge panel in Arjun Panditrao Khotkar v Kailash Kishanrao Goratyal (known as "Arjun v Kailash") has now defined how Section 65B should be interpreted. Confusion emerged regarding the intent and application of Section 65B due to conflicting opinions expressed in three prior Supreme Court rulings – in ***Anvar P.V. v P.K. Basheer***[12] ('Anvar v Basheer'), ***Shahfi Mohammad v State of Himachal Pradesh***[13] ('Shahfi Mohammad') and ***Tomaso Bruno v State of Uttar Pradesh***[14] ('Tomaso Bruno').[15]

Section 65B of the Evidence Act provides for the admissibility of electronic records. This

[11] Indian Evidence Act, 1872, s 66
[12] *Anvar P.V v P.K Basheer* (2014) 10 SCC 473
[13] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801
[14] *Tomaso Bruno & Arv v State of U.P* (2015) 7 SCC 178
[15] Bharat Vasani & Varun Kannan, 'Supreme Court on the admissibility of electronic evidence under Section 65B of the Evidence Act' (*Cyril Amarchand Mangaldas Blog*, 16 August 2021) <https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/> accessed 16 July 2022

section states that any information contained in an electronic record that is printed, stored, recorded, or copied on optical or magnetic media as a result of a computer (referred to as computer output) shall be deemed a document. If the conditions outlined in this section are met with regard to the information and the computer in question, the document would be deemed admissible in court.

The conditions for any computer output to be deemed admissible under Section 65B(1) of the Indian Evidence Act are as follows:

a) the computer which was used to obtain the information produced by it should have been under regular use i.e. in subsequent usage for storing or recording data in its daily course of action operated under the lawful controller of the computer.
b) during the said period, the information stored and recorded on the computer and the output derived from it was fed into the system in the ordinary course of the said activities.
c) the computer used to store or record data, during the said period of time, was working properly, and if any failure in the system during any period did not affect the electronic record or the accuracy of its contents.
d) The data in the electronic record replicates or is generated from the data entered into the computer normally when performing the aforementioned operations.[16]

A certificate may be produced, according to the law, if the requirements outlined in the previous sub-section (2) of Section 65B of the Indian Evidence Act are met. The certificate's purpose is to both identify the electronic record that contains the statement and explain how it was created must provide details on any equipment used in the creation of that electronic document to address any issues related to the circumstances listed in the sub-section (2). A person holding a responsible position with respect to the equipment via which the data has been created must sign the certificate. The addition of this section was to make the evidence more reliable and readier for interpretation by the court even on non-technical grounds.

[16] Indian Evidence Act, 1872, s 65B(2)

The court is subjected to a lot of challenges when dealing with electronic evidence and adjudicating upon the admissibility of electronic records because of their uncertain genuineness, veracity, and reliability to steer the outcomes of the case. The technical nature of the electronic evidence requires scrutiny by experts in that field and that details to be worked out in a way comprehensible by both the court and the representatives of the parties concerned. Some clauses of the law stand conflicting with each other and there does not appear a clear scope for considering the various interpretation of the clause. As in the statement of objects of the IT Act, the purpose was to make electronic records as a shred of evidence along with the already existing paper-based and oral evidence. It translates that print-outs do not fall under the expressions of the term "electronic record". However, Section 65B(2) of the Indian Evidence Act, also includes electronic records made out into a printed paper-based output.[17] There is also a need for safeguards to protect the privacy and confidentiality of the contents recorded in such evidence. Section 65B was amended by the Information Technology Act, however, the interpretation of its clauses was kept hanging at the discretion of the court and its circumstances. The contradicting judgements regarding the same have only added to the challenges.

DISCUSSION AND RESEARCH FINDINGS

- ***Admissibility of illegally extracted chats***

In the current scenario, India does not have a law ruling on the protection of data privacy. The right to privacy is a crucial component that supports persons' other fundamental rights, including their right to life. In ***Justice K.S. Puttaswamy (Retd.) v Union of India***, the right to privacy—which was regarded as a basic right—arose principally from Article 21 of the Indian Constitution.[18]

The state must establish a data protection system that supports the general welfare while

[17] Shobha Gupta, Why is admissibility and authenticity of electronic evidence necessary?(*The Leaflet*, 17 August 2021) <https://www.theleaflet.in/why-is-admissibility-and-authenticity-of-electronic-evidence-complicated/> accessed 16 July 2022

[18] *Justice K.S. Puttaswamy v Union of India* 2017) 10 SCC 1

safeguarding citizens against threats to their informational privacy coming from both state and non-state actors in order for this right to have any real value. While developing a data protection framework, the Committee must keep in mind the state's obligations. Even when there is an absence of codified law regarding the matters of data privacy, the relevant laws under the Information Technology Act, 2000, and the Contract Act, 1872 fill in the void for the protection of data of individuals. Sections 72 and 72A of the Information Technology Act, 2000 safeguard the data of any individual available with corporations or organizations who holds the power of possessing, storing, transmitting, and handling of such from sharing such information with any individual or organization and penalizes them with fines and imprisonment for non-compliance. However, Section 69 of the IT Act provides an exception to the general rule of maintaining information privacy and secrecy, allowing the state or central government to intercept or monitor data if it is in the interest of the sovereign or integrity of India, defence of India, security of the State, friendly relations with the foreign states, or public order, as well as for preventing incitement to the commission of any cognizable offence relating to previous or for these purposes. A contrast can be drawn between the law on the admissibility of illegally extracted evidence between India and the US to conclude where Indian law stands on the topic in question. The United States Constitution and Bill of Rights do not specifically include a right to privacy. The Amendments that came after the Third Amendment threw light upon the safeguarding of the privacy of individuals. While in the United States, illegally extracted evidence was deemed inadmissible due to the application of the exclusionary principle and the doctrine of 'Fruits of Poisonous Tree'. This judge-made regulation is intended to prevent law enforcement officials from carrying out searches or seizures that are against the Fourth Amendment's prohibition against unreasonable searches and seizures and to give defendants who have had their rights violated recourse. Evidence that was later collected by a legitimate search and seizure may be considered acceptable even though it was first obtained illegally. In the Indian scenario, it is a burning question whether the privacy of citizens should be allowed to be violated in the process of acquiring information that may convict them as criminals. In ***Justice K.S. Puttaswamy v Union of India***, where the national identity project, the Aadhaar project, was challenged, a larger panel of nine judges

concluded in 2017 that the right to privacy is a fundamental right and is safeguarded by Articles 14, 19, and 21. This significant decision reversed the last two rulings and concluded that any violation of a basic right must be justified by a legal standard requiring a just, fair, and reasonable approach. In the ***State of Maharashtra v Natwarlal Damodardas Soni***[19], the Anti-Corruption Bureau seized gold biscuits unaccounted for by the respondent. In his absence, the bureau of police and the customs authorities reached the house of the respondent and enacted a search and seizure. The respondent was detained on serious smuggling allegations. According to the court, rejecting the respondent's appeal regarding the illegal search, "assuming that the search was illegal, it would not affect either the validity of the seizure and subsequent investigation by the Customs Authorities or the validity of the trial that followed on the complaint of the Assistant Collector of Customs."

Evidence Act allows admission of data on the basis of relevancy. Illegally extracted chats are considered as much evidence as any legally obtained document because the law tests for the relevancy of the evidence to the facts in issue.

Whether the original digital document is admissible as primary evidence without applying Section 65B

Admissibility of the document can only be made possible if the contents of the document are proven by primary evidence except for some cases where secondary evidence may also be given to establishing the facts as mentioned in sections 64 and 65 respectively of the Indian Evidence Act. Special provisions were made with amendments to section 65 of the Evidence Act, as per the introduction of the Information Technology Act, 2000, which stated that electronic records may be proven in accordance with the subsequent section. The word "electronic record" refers to data, records, or data created, images or sounds saved, received, or communicated in electronic form, as well as microfilm or computer-generated microfiche, as defined by Section 2(1)(t) of the IT Act. Ordinary paper-based records are specifically superseded by electronic records under Section 4 of the IT Act. There has been a conundrum regarding the necessity of filing a certificate of authenticity issued by the respective experts as

[19] *State of Maharashtra v Natwarlal Damodardas Soni* (1980), AIR 593

mentioned in u/s 65B(4) after the conditions mentioned in u/s 65B(2) are duly satisfied and whether Section 65B can override the provisions of Sections 63 and 65 to be deemed admissible in the court of law. In ***State (NCT of Delhi) v Navjot Sandhu @ Afzal Guru***, the Supreme Court ruled that introducing secondary evidence under Sections 63 and 65 of the Evidence Act is not prohibited, regardless of whether Section 65B of the Evidence Act, which deals with the admissibility of electronic records, has been complied with. Additionally, it was decided that even in the absence of a certificate meeting the requirements of subsection (2) of section 65B of the Evidence Act, such electronic evidence might still be admitted into a court case. This was however overruled in the case of ***Anvar PV v P.K Basheer & Ors***, which held conclusively that electronic records can only be proven by the conditions mentioned u/s 65B(2) of the Evidence Act and that a certificate under sub-section (4) is mandatory for validating that the conditions mentioned in sub-section (2) were followed. In the following case of ***Tomaso Bruno v State of Uttar Pradesh***, the three-judge bench of the Supreme Court held that secondary evidence of the contents of a document can be led under Section 65. The judgement on the case, however, never relied on section 65B(4) nor made a precedent of Anvar (supra) but specifically relied on Navjot Sandhu (supra). The Supreme Court ruled in ***Shafhi Mohammad v State of Himachal Pradesh*** that Section 65B procedural and not necessarily obligatory obligation to provide a certificate is true. A certificate pursuant to Section 65B may not be demanded from a party who is not in possession of the equipment from which the document is created (4). The procedural requirement set forth in Section 65B(4), according to the Court, should only be applied where electronic evidence is produced by a person who is in command of the necessary tools and is thus qualified to do so. If the person is not in possession of the equipment, Sections 63 and 65 cannot be ignored.[20]

[20] Aditya Mehta & Co., 'Section 65B of the Indian Evidence Act, 1872: Requirements for admissibility of electronic evidence revisited by the Supreme Court, India Corporate Law' (Cyril Amarchand Mangaldas Blog, 18 August 2021) <https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/#_ftnref4> accessed 16 July 2022

The Supreme Court of India therein intervened and dealt with the following decision and clarified the position:

(a) The acceptance of any electronic record as evidence is subject to the certificate required by section 65B(4) of the Evidence Act.

(b) Section 65B(1) begins with a non-obstante clause that states that only if the requirements outlined in sections 65B(2) and (4) are met may documentary evidence in the form of electronic data be proven and declared admissible. Sections 62 and 65 are unimportant since this is a specific provision.

(c) The certificate cannot be replaced by oral evidence as described in Section 63(5), and the person in charge of a computer system cannot provide evidence in lieu of the necessary certificate.

(d) The certificate may be shown at any moment throughout the trial.

(e) If the computer itself is presented for examination, the certificate is not required. The computer is the document's original source. This is possible if the owner himself enters the witness stand and affirms that he is the one who owns and operates the business. However, if the electronic record is connected to a network, the only method to offer it is in accordance with S. 65B (1) and 65B. (4).

Whether WhatsApp chats are admissible in a court of law

Technological advancements have led to faster communication and connection between individuals. Millions of conversations are held over the internet in a fraction of a second. WhatsApp, a product born out of this revolution, is one of the leading applications that facilitates user-to-user encrypted instant messaging services. With WhatsApp becoming the all prevailing medium of communication, corporations are shifting their paradigm of communication with customers to a flexible WhatsApp chat to answer their queries. Since most of the conversations are held over this platform it has indubitably become a very important source from the evidentiary point of view and the question of whether WhatsApp

chats are admissible in a court of law is more relevant than ever. WhatsApp chats fall under the definition of electronic records stated under section 2(1)(t) of the Information Technology Act as data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated microfiche. WhatsApp chats are considered secondary in nature because only the print-out of such chats is presented in the court as evidence if the original electronic device such as the mobile phone or computer is not available for review. The amendment of the Evidence Act in 2000, with the introduction of the Information Technology Act, established special provisions, which are complete in themselves, as sections 65A and 65B which provided the criteria for admissibility of electronic records as evidence. The confusion regarding the requirement of a certificate as per section 65B(4) was cleared by the Supreme Court of India in its 2020 judgement of the ***Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal***, where it was held that section 65B(4) is a condition precedent, however, if the owner presents the original source, i.e. the mobile phone or the computer, and declares the authenticity of the document, then the condition under section 65B(4) can be overlooked. Apart from the conditions which are to be fulfilled under section 65B(2), WhatsApp chats are also required to satisfy these conditions before being deemed admissible; (a) Recipient should have received the message intended to him, i.e. in the context of WhatsApp, double ticks for the concerned message. (b) The phone should be in perfect condition and in regular use during the course of receiving the message. (c) The sender should have the intention to send those messages. WhatsApp enables the sender of a message to confirm the successful sending and reading of the message by the recipient through a feature of double ticks and blue ticks. A double tick on sent messages indicates that the message was received by the recipient and a subsequent double blue tick indicates that the message was successfully read by the recipient. The Bombay High Court's 2018 ruling in SBI Cards and ***Installment Administrations Pvt. Ltd. v Rohit Jadhav***, where it was noted that the defaulter had received and read the notification through WhatsApp, was strengthened by this feature of the messaging app. The court decided that if a blue tick appears following the transmission of a message via WhatsApp, the informative application is seen as reliable proof that the recipient of the message really received it.

In ***Ambalal Sarabhai Enterprise Ltd. v KS Infraspace LLP Ltd.,***[21] the Supreme Court has referred to WhatsApp chats as evidence and said that "the WhatsApp messages which are virtual verbal communications are a matter of evidence with regard to their meaning and its content to be proved during the trial by evidence in chief and cross-examination". In many other court precedents, like in ***Rajesh Kumar Singla v Union of India***[22], WhatsApp chats were relied upon for granting bail in an NDPS Case and the court also made clear that without presenting the certificate as mentioned u/s 65B(4) of the Evidence Act, WhatsApp chats cannot be admissible as evidence. Similarly, the High Court of Gujrat granted bail on the basis of WhatsApp chats in ***Chirag Dipakbhai Sulekha v State of Gujrat.***[23] WhatsApp has transformed into a verb today and its possibilities in the internet sphere are ever-expanding. From the aforementioned explanation of the facts and the precedent judgements, it is clear that WhatsApp chats are secondary in nature (since only the photocopies of the chats can be presented) and only when accompanied by the certificate mentioned u/s 65B(4) and fulfilling of the conditions mentioned u/s 65B(2), is when the chats are deemed admissible in the court of law. Since there is a shift from the traditional paper-based evidence to a more electronic form and there is a need to further reform the laws governing the admissibility and interpretation of electronic records as evidence.

CONCLUSION

Technology has inevitably become an extended part of our society. There has been an overwhelming number of opportunities and challenges amidst the technological revolution in all fields of human work. Technology has paved the way for a faster, more transparent, and efficient system of getting things done. Corporations are turning to digital mediums to survive and thrive in this era. The Information Act of 2000, together with the Evidence Act's ensuing changes, made a significant impact on the Indian judicial system by laying down the conditions for the acceptance of electronic documents as evidence in courtrooms, which were previously controlled by sections 62 to 64. The evidentiary value of any document could only

[21] *Ambalal Sarabhai Enterprise Ltd. v KS Infraspace LLP Limited and Another* (2019) Civil Appeal No. 9346/2019
[22] *Rajesh Kumar Singla v Union of India* (2020) CRM-M No. 23220/2020
[23] *Chirag Dipakbhai Sulekha v State of Gujarat* (2020) Criminal Misc. Application No. 18834/2020

be evaluated by its relevancy of it to the facts in the issue. The court refuted the appeal of the respondent for an illegal search and seizure and legality of the evidence and held that even if the search was to be assumed illegal it does not affect the relevancy of the evidence. The interception of data was called on the basis of whether such data was against the sovereignty of the state, an imminent threat to the state, and as such which an exception to general maintenance and secrecy of information as mentioned in section 69 of the IT Act. The newly amended sections 65A and 65B of the evidence established the rules for the admissibility of electronic records. The interpretation of the sub-section (4) of this section was however unclear and the conflicting judgements on this issue gave rise to many questions. This air was cleared in the instant case of Arjun Panditrao Khotkar, where the Supreme Court held that certificate, after fulfillment of the conditions made available in sub-section (2), under sub-section (4) is mandatory for an electronic record to be deemed admissible. These are special provisions and therefore sections 62 and 65 are irrelevant It was also held that if the owner/operator itself presents the device/mobile phone/computer in the court for analysis and declares the same in the witness box, the condition for the certificate is held no longer necessary. The instant messaging phenomenon brought about by the encrypted messaging application; WhatsApp brought about questions regarding the admissibility of the contents of a chat in a court of law. Since only the printed copies of the chats could be brought to the presence of the court therefore it was to be considered to be secondary evidence under section 65B(1). Cases like in Rajesh Kumar Singla bail was given relying on WhatsApp chat, however, it was also held that without the certificate as mentioned u/s 65B(4), it cannot be deemed admissible in the court. The recent breach of electronic evidence (in the form of WhatsApp chats) underlines the necessity for measures to be put in place to preserve and keep electronic records in addition to the practical challenges. It may be required to produce a certificate in accordance with Section 65B(4) to verify authenticity, but additional measures must also be taken to preserve the privacy and confidentiality of the data contained in electronic records. A five-judge committee's report from November 2018 that contained draught rules for the preservation, retrieval, and authentication of electronic documents was cited by Justice Nariman in his ruling.