

ELECTRONIC EVIDENCE: AN OVER VIEW OF CALL DATA RECORDS, THE CDRS

Dr AK Vashishta*

Abstract

Advent of the Information technology has influenced every facet of life on the planet. It is so integral to the day-to-day activities that it goes without saying that there is no part of human life which is not influenced by the inroads made in the field of electronics. One remarkable impact which, for a student of Law, it has caused is in the field of evidence in criminal trials. By student we understand anyone in the great field of the practice of Law whether a judge, an advocate or a jurist. Electronics have encompassed all conceivable fields by using available vehicles viz., SMS, MMS, Whatsapp, twitter, Instagram, audio calls, video conversations etc. What was a fancy once upon a time is as simple as breathing today? In fact, like the life support systems working in the body of their own will, appear so simple but their processes are so complex that when a little goes awry, it takes expert's help to put it back on track. Similar to these is the use of electronics in our lives. Looking at everything with a contemplative eye, for the benefit of all and sundry, we propound a theory which forms basis for future deductions and becomes a subject matter of intense interest.

* Ex Dean Maharishi Law School, is a practicing lawyer at Delhi High Court and is also member of the International Council of Jurists London and Peer Reviewer from India for commentaries on Geneva Convention IV, appointed by the Hague Office of ICRC.

Na mantram no yantram tadapi cha na jane stuti katha !

**(I know no hymns, no rhymes nor am I familiar with lofty eulogies that I can say in
praise of you)**

-Adi Sankara¹

INTRODUCTION

Advent of the Information Technology has influenced every facet of life on the planet. It is so integral to the day to day activities that it goes without saying that there is no part of human life which is not influenced by the inroads made in the field of electronics. One remarkable impact which, for a student of Law, it has caused is in the field of evidence in criminal trials. By student we understand anyone in the great field of the practice of Law whether a Judge, an Advocate or a Jurist. Electronics have encompassed all conceivable fields by using available vehicles viz., SMS, MMS, WhatsApp, Twitter, Instagram, audio calls, video conversations etc. What was a fancy once upon a time is as simple as breathing today. In fact like the life support systems working in the body of their own will, appear so simple but their processes are so complex that when a little goes awry, it takes expert's help to put it back on track. Similar to these is the use of electronics in our lives. Looking at everything with a contemplative eye, for the benefit of all and sundry, we propound a theory which forms basis for future deductions and becomes a subject matter of intense interest.

THE CALL DATA RECORDS - THE CDRS FOR SHORT

Relevance of electronic evidence in criminal trials is gaining importance with every passing day. Fortunately, the field is not yet so open for the concept of the conflict of laws and thus comfortably traverses the turf of the *lex loci actus* without much ado. The lawyer's profound wit is what determines its juristic propensity. It is often heard at the Bar that this new law is the Prosecutor's code. Of course it is, but merrily, no law is ever lopsided. In fact any law with lopsided trappings would not survive the test of consistency, repugnancy and derogation under Article 13 of the Constitution. Our attention is unwittingly drawn towards the recordings of the Constituent Assembly Debates and we realise the exceptional farsightedness of the framers of our Constitution.

Let this be examined as to what happens at the trials generally when the electronic evidence is brought in or is intended to be brought in. During criminal trials, it comes to notice that where

¹Adi Sankara in Apradha kshamapan Stotram – an invocation in praise of the Lord Goddess Kalika

evidence is of a nature where the transaction or the fact in issue is beyond tangible human control like conversations on electronic media, or voice calls where the voice has been thrown in the space through a medium which cannot by ordinary course retrieve what has been said and the same becomes the fact in issue, the Investigating Agencies heavily rely upon the tried and tested retrieval methods, applicable to the Electronic Evidence. The field is the prime focus of continuous research of the superlative engineering genius. Reverting to the evidence proper, the simplest but one of the most potent and illustrative example is of oral conversations by use of telephones, through mobile telephones or the land line connections. If we take the example of telephone calls, which is the commonest mode of communication, the Investigating Agencies ordinarily ask for the Call Data Records known as CDR for short. These are obtained from the agency holding information, by the end user, through three different conventional mediums viz, through fax, through normal post or through the scanned letters by e-mail. The caution for a Judge is that every single piece of evidence ought to be seen through the prism of the guidelines laid down in the Law of Evidence. Now, with a view to understand this complexity, we take the example of calls made from and received into cellular phones of two different individuals.

THE LAW ON THE SUBJECT

Important to understand is as to what are Sections 65 A and 65 B of Indian Evidence Act. Section 65 A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B. Section 65B lays down the conditions which are essential to be fulfilled while considering the admissibility of electronic records. The provisions apply in the case of telephone records as well and thus read as follows:-

“65B Admissibility of electronic records. *(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.*

(2) The conditions referred to in Sub-section (1) in respect of a computer output shall be the following, namely:-

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;*
 - (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;*
 - (c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and*
 - (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.*
- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in Clause (a) of Sub-section (2) was regularly performed by computers, whether-*
- (a) by a combination of computers operating over that period; or*
 - (b) by different computers operating in succession over that period; or*
 - (c) by different combinations of computers operating in succession over that period; or*
 - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,*
- all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in the section to a computer shall be construed accordingly.*
- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-*
- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;*

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in Sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.”

The thumb rule in this field is that certain electromagnetic devices are ‘document’ for the sake of evidence. The essential point is that the electronic records cannot be accepted in evidence in any form unless the guidelines contained in Section 65 B of the Indian Evidence Act have been fully complied with. What the court has to determine is whether the electronic records produced pass the test of Section 65 B. The section prescribes the mode for proof of contents of electronic records. The primary purpose is to sanctify proof by Secondary Evidence. This facility of proof by Secondary Evidence would apply to any computer output, such output being deemed as a document. Section 3 of the Evidence Act defines a ‘document’ which means “any matter expressed or described upon any substance by means of letter, figures or marks or by more than one of those means, intended to be used, or which may be used, for the purpose of recording

that matter.” For instance, writing is a Document. Similarly, electronic record is defined in Section 3 of Evidence Act. Section 3 Evidence Act states that the expression ‘electronic record’ has the same meaning as attributed to it in the IT Act. Section 2(t) of the IT Act defines ‘electronic record’ to mean: “(t) electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.”

The conditions prerequisite with respect to its relevancy and admissibility are as given in Sub-section (2) of sec 65 B. Take an example of production of CDRs from the servers of an agency under the control directly or indirectly, of the State, which are stored in the designated hard disk of the computer/ system and downloaded from it (on demand), for the purpose of evidence, a certificate mandated by Sub-section (4) of section 65 B is then required to be placed before the Court to which the Court is required to give a careful consideration. For instance, the certificate which is eventually attached as an Exhibit to the trial proceedings, has been signed by an officer superior to the Nodal Officer from the same office, say one of the Divisional Engineers of the service provider. Should he be competent to issue the said certificate by virtue of his seniority? Sub-section (4) lays down that the certificate is to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the activities whichever is appropriate. If this requirement is met, it shall be considered as evidence of any matter stated in the certificate and shall be sufficient to meet the requirement of Section 65 B.

WHAT IS PROSECUTION, IF IT IS THE PARTY ADDUCING EVIDENCE, REQUIRED TO DO?

To begin with, in a criminal trial, the Prosecution has to admit and concede that the information required to be produced as evidence is contained on an electronic medium. It (the Prosecution) has to further surrender itself to the legal position that the records copied on electromagnetic media cannot be admitted in evidence unless and until the pre-requisite conditions as stipulated under Sections 65 A and 65 B of Indian Evidence Act, have been fully met. Therefore, the statements made by Prosecution Witnesses deposing in relation to the evidence admissible under Section 65, during the Examination in Chief, have to pass the dual tests of correctness and propriety. These tests are not only with respect to the competency of the witness to testify and the evidence to be admissible but also with respect to the propriety of the position of the person appearing under the cloak of Nodal Officer. Next is the issue of the authority vested in that

officer who must be at the relevant time posted at the relevant place in the office of the service provider who could be a State agency like Bharat Sanchar Nigam Limited, or any other private operator. It also remains an admitted fact that in Electronic Evidence, a certificate issued by the Nodal officer meeting the requirements of clause 4 of Section 65 B of the Indian Evidence Act, is mandatory.

An invariable contention, which is raised by the parties to the proceedings or a suit is, that the documents which are in the form of certificate or the Call Data Records are not conforming to the requirements of Section 65 of the Evidence Act and thus an argument of the party to the contrary is far from truth. This kind of a situation arises in a trial or a suit when a party to the suit or the proceedings contends an anomaly that the impugned CDRs are unauthenticated since those were acquired having been issued on a date without any certificate by the Nodal Officer or that the data is open to tampering and thus unreliable from the source. Adding strength to the counter contentions on the admissibility, it is also contended that *no authority other than the Nodal Officer at the relevant time* could have issued the mandated certificate as he alone possesses the expertise as well as the authority to do so under the Act.

Sometimes an argument is taken that perusal of impugned CDRs which are originated by the Nodal Officer of a service provider, proves that only a specified number of attachments were sent by/received from the service provider and the certificate provided by Section 65B was not one of the attachments. The argument is considered frivolous since the other attachments have originated from the designated service provider derived in the due course of business but is definitely contentious, as a person in a whirlpool, revolving in incessant uncertainty, shall pull every straw to the centre! When the verity of the received attachments is challenged by the opposing party on the ground of admissibility, the necessary certificate assumes importance.

In the process of acquisition of information, the Investigating Agency addresses a letter to the Nodal Officer requesting for the CDRs. On compliance of this request, the Nodal Officer supplies a Compact Disc and the transcript of the conversations written on the CD. Sometimes, dissimilarities are observed in the content in the nature of different font etc., if a set of transcript was taken at the initial stages of investigation and another set is obtained at a later date. These are miniscule but give a good ground for a contention. Being of utmost sensitive nature, these are treated as the two different sets of CDRs though containing the details of the same records. The Judge has to deal with it with patience as both parties, the one producing and the other contesting apply all vehemence to their respective points of view. It is a piquant situation which

requires dexterous handling by the party producing the evidence which is normally the prosecution in a criminal trial.

How should the Prosecution overcome this pithole? The Prosecution or the party producing the CDRs would hold steadfast on the genuineness of its evidence and shall insist on admissibility but a sensible protagonist would also graciously concede an argument in such situations and support a viewpoint limited only to the extent that there are bound to be dissimilarities when two print outs are taken. But the content being inscribed on a CD has the facility to match with the transcript on the print outs. The logic forwarded in support of the dissimilarities, is, not very convincing and is generally accepted with a pinch of salt. In any case, any logic would then, may noy straighten out this bulge. It is still good to make such an argument but nobody will buy it because once a document is sent, say on the e-mail, its font cannot be changed without the interpolations being recorded in the backup and retrievable at will by an expert. The rule is that changes are not with in the purview of the receiver and the contents will remain the same. If there is a change, it becomes inadmissible in evidence. Once the Prosecution concedes a change, it becomes inadmissible. Another important point is, the seniority in hierarchy of the service provider is not the determinant factor for competence i.e., an officer of the service provider cannot assume authority of a Nodal Officer under Section 65 B just because he is senior to the rest. Authority actually flows from the appointment as Nodal Officer. Since the latter is required to depose about the verity of system, the contents of the certificate with regard to the condition of the servers also becomes misleading, if statement has been made merely on the basis of seniority in status - only the then Nodal Officer can make such a statement. Once having contended that there are differences between Exhibits, the Prosecution cannot contend that authority of certain exhibits stands confirmed while in respect of others it does not.

THE COUNTER CONTENTIONS

In all cases, the counter party if it is the Defence or the Respondent, raises an important issue of admissibility of the electronic records, say the CDRs being not in conformity with the requirements of Section 65 B of the Indian Evidence Act. The contentions are generally focused on-

- (a) The CDRs produced in the Court as Exhibits are not signed by the Nodal Officer of the service provider;

- (b) party producing the electronic records fails to produce the certificate mandated under Section 65 B of the Indian Evidence Act;
- (c) the certificate given under Section 65 B of the Indian Evidence Act, is not signed by the Nodal Officer. Instead it is rendered improperly and without authority;
- (d) the certificate rendered is false since it is postdated while the CDRs relate to the period prior to its issue;
- (e) the authority letter is prepared prior to the certificate under Section 65 B of the Indian Evidence Act;
- (f) the witness is not the Nodal Officer hence, is not the competent authority to affix his signature on the CDRs;
- (g) electronic records have been tampered to suit the requirement of the party producing them hence, the records produced must be rejected;
- (h) since there is a mandatory requirement to nominate a Nodal Officer who is authorized to download the data say for issuing CDRs and issue certified copy thereof, he alone possesses the “required Key.” This fact is ignored by the party producing and relying on electronic evidence;
- (i) data is supplied by officer not holding the post of Nodal Officer;
- (j) the record produced is not maintained in ordinary course of business stored in the designated hard disk of the computer system of the service provider. Hence the record is inadmissible being not free from any doubt;
- (k) unique User-ID and Password were available to more than one person providing access to the data stored was to those other than the only designated officials;
- (l) conditions of Section 65 (2) of the Indian Evidence Act have also not been complied with since the data has been interpolated and thus cannot be considered to have been created in usual and ordinary course of business;

As far as the awareness goes, the counter party challenges the competency of such superior officer to render the said certificate. The Court in that case needs to satisfy whether the officer

superior to the Nodal Officer of the service provider could be considered as competent in terms of Section 65 B(4) of the Indian Evidence Act.

Sometimes, Junior Telecom Officers produce copies of the office orders authorizing them to provide call details to the Investigating Agencies or even to the Trial Courts on Summons. This approach is vehemently contested on the ground that the officer is not a Nodal Officer and since the superior officer too, is not the competent authority in this regard, the office order is devoid of legal force.

When the testimony of a witness discloses that data had been stored in the electronic system of the service provider, and down loaded by the Nodal Officer on a requisition of a party to a suit or proceedings, in due course of business, and this fact has been brought on record incontrovertibly, it now rests in the wisdom of the court to decipher whether in its opinion it meets the requirements of Section 65 B of the Indian Evidence Act or not.

Wisdom of the high seat of justice

Showing the way in this complex field of specialised knowledge, the Supreme Court of India, dwelt upon this issue in the case of J. Yashodha v. K Shobha Rani², and observed that only the best evidence which the nature of the case will admit shall be produced. The other case on the subject is the State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru³. Here the importance of producing the necessary certificate under Section 65 B and the required key is discussed. Since there is a mandatory requirement to nominate a Nodal Officer who is authorised to download for issuing CDRs and issue certified copy, he alone possesses the “required Key”. Not to leave behind is Anwar P.V. v. P. K. Basbeer⁴, wherein the issue of admissibility of Electronic Evidence in a judicial proceeding has been revisited and reiterated and determined.

The latest position is given by the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal decided on 14 July, 2020 wherein the Court discussed their own decision of a two Judges Bench in Shafi Mohammad v. State of Himachal Pradesh⁵. The Court went through a catena of decisions, Indian and foreign, quoting a few, viz., Ram Singh v. Ram Singh⁶, - a three-Judge Bench decision; R. v. Maqsood Ali⁷, and R. v. Robson⁸, to conclude to the effect that it would be wrong to

² 2007 (5) SCC 730

³ 2003(6) SCC 64

⁴ 2014 (10) SCC 473

⁵ (2018) 2 SCC 801

⁶ 1985 Supp. SCC 611

⁷ (1966) 1 QB 688

⁸ (1972) 1 WLR 651

deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved. Such evidence should always be regarded with some caution and assessed in the light of the circumstances of each case. Electronic Evidence is thus held admissible subject to safeguards adopted by the Court about its authenticity. Taking the case of tape- recording, the voice of the speaker must be duly identified. Equally important is the accuracy of the statement made therein. Which is required to be proved by the maker of the record from where, any possibility of tampering is required to be ruled out. Thus the reliability of the piece of evidence is certainly a matter to be determined in the facts and circumstances of a fact situation. Now about the threshold admissibility of the Electronic Evidence, it cannot be ruled out on any technicality if the piece of evidence is relevant.

Indeed the scientific temper must be allowed to pervade the method of investigation where the Electronic Evidence is relevant to establish the alleged facts. It is of immense help to the Investigating Agency. A reference is also made to the order of the Supreme Court in *Mohd. Kasab v. State of Maharashtra*⁹.

HOW SHOULD THE TRIAL JUDGE HANDLE THIS?

As would be the case generally, if certain Exhibits are issued by a Nodal Officer and produced before the Trial Judge as authentic documents those are presumed to be so. That is as far as the admissibility is concerned. Once having crossed this first hurdle, every Nodal Officer issuing a certificate under Section 65 B of the Indian Evidence Act is required to know and depose about his awareness of the provisions of the said Section. Contents are a matter of merit and are dealt with separately. Therefore, the learned Judge has to exercise restraint in remarks and deductions and patience in examination before admitting. There is no doubt left now that Section 65 B stipulates certain mandatory conditions given in the Section to be satisfied before any Electronic Evidence is admitted in evidence. Amongst others, there is a requirement of a certificate to be rendered in accordance with Sub-Section (4) of 65 B. The certificate should be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.

While interpreting the provisions of Section 65B, it would be apt to refer and recount the remarks of Hon'ble Mr Justice Rajendra Menon, the Chairperson of the Armed Forces Tribunal,

⁹ (2012) 9 SCC 1

New Delhi, India, in the judgement and order in the Original Application OA No 1063 of 2021, Lt Col Ranjit Singh v. Union of India & Others, decided on 27th Oct 2021, “.....*another principle, cardinal in nature in the matter of construing a statutory provision is that a statute must be construed to make it effective and workable. Anything done or to lien against a construction, which reduces a statute to a futility, should always be avoided. While doing so, regard should be had with regard to the subject and object proposed to be achieved by the statute.*”

Maintaining absolute impartiality and objectivity in approach, for what purpose the CDRs are maintained must be asked. What procedure does the office of the service provider follow when approached for CDRs through an official requisition duly signed by a competent authority of that agency, is what the Trial Judge is required to elicit from the Nodal Officer appearing as a witness in the Court? The learned Judge must not forget his onerous responsibility to take essential details on record, irrespective of the fact which party is producing the witness. CDRs are actually maintained as a part of license agreement between Department of Telecom and the service provider. It is maintained to provide a record for sasecurity agencies for a period of one year after which it is automatically deleted from the CDR server located at Nodal Centre. Nodal Officer then accesses the CDR stored at the Nodal Centre, through a specific portal using a specific log- in- id and password. Then the CDR is downloaded and stored in the hard disk of the computer. After this it is sent by e-mail as a text file as an attachment to the requisitioning authority.

WHAT ARE THE SAFEGUARDS TO ENSURE THAT THE DATA CANNOT BE TAMPERED WITH?

The mail account for instance xmail.CDR@gmail.com which as a hypothesis could be the official mail id of Nodal Officer dealing with security related issues, is accessed only by the officer authorized- none other than the Nodal Officer himself. This is one protection which ensures that server is not accessed by any wayward operator. The data stored in the server is auto protected by the locking devices generated by the system software as auto safeguard and thus cannot be tampered with. It is only when once the e-mail attachment is downloaded by the user-authorized user of the service provider, he can tamper with it on the computer he is using, and thereafter load and send it, but the date of the document will then be the date on which it was sent. This can be traced and interpolations can be deciphered. Further detailed analysis of data device would reveal all the stages through which and the devices on which the data has been

processed. The intense and incisive judicial contemplation is what is required from the Trial Judge at this stage to separate the grain from the chaff.

As a security measure, some service providers in fact use two different User Names and Passwords to obtain CDRs. One User Name is utilized to access the official e-mail id and the second Username and Password is used for accessing CDR from the server. Nodal Officer is required to be aware of both the IDs.

It's the Court which eventually determines that requirements of Sub-section (4) of Section 65 B have been met and that, thus, has no illegality in it. The light at the horizon is the rays of judicial and juristic reflections in the form of judgements and orders. The wisdom of the final arbiter, the Supreme Court is the beacon and it is there like the light house showing way to every ship!