

# Procedural Pitfalls & Enforcement Challenges

*N. S. Nappinai*

*Advocate*

[nappinai@nappinai.com](mailto:nappinai@nappinai.com)

*Founder Member – Technology Law Forum*

# Issues & Concerns

- Electronic Evidence:  
Authenticity, Integrity & Non –  
Repudiation;
- Jurisdiction – Civil & Criminal;
- Enforcement: Implementing &  
Enforcing Orders;

# Primary challenges to Electronic Evidence

- In Collation, Retention, Evaluation & Appreciation of Electronic Evidence:
- Authenticity:
  - Of Author – hand is no longer attached to you;
  - Electronic & Digital Signatures – how safe is it?;
- Integrity:
  - How tamper proof is it?
  - Ease of tampering Vs. proof of tampering;
- Non-repudiation:
  - Binding nature of evidence;
  - Onus – where does it lie?

# Electronic Vs. Paper

- In the “real” world an “original” – is one (including Counterparts, if any);
- In the “virtual” world - Every Copy is an “original”;
- Death of an Original in the Real world – slow & steady most times;
- Death in the Electronic World – two extremes – Now its there – now its gone! Or it never dies – especially when you want it to!!! On the Net!

# First Principles & Electronic Evidence

- What is the nature of document / Electronic Record;
- Author & Recipient - Where, What, Who, When, How;
- Chain of custody – from author till production;
- Proof – of document & Contents;
- Authenticity & integrity of Document / Electronic Record;

# Signature & Electronic signatures

- When did you last use an electronic signature?
- How is it different from a digital signature?
- “In Witness whereof we the undersigned have set our hand on this the \_\_\_\_\_ day of \_\_\_\_\_”
- Signatures:
  - Uniqueness;
  - Detection of alteration;
  - linked to paper;
  - Linked to person;

# Evidence & Electronic Evidence

- General Laws:
  - Indian Evidence Act;
  - Indian Penal Code;
- Special Enactment:
  - Information Technology Act, 2000;
- Implications & Issues:
  - New wine in an Old Bottle?
  - Dynamism of Law;
  - Purposive Interpretation
  - Real Vs. Virtual world – Is there any difference to our approach?
  - Pitfalls in the investigative process in dealing with Electronic Records;
  - Judicial recognition of electronic records;



# Electronic Evidence - Proving

- Happily ever after?
- Electronic Evidence – documents, their collation & proving;
- Electronic Evidence – the bread trail;
- Electronic Evidence – appreciation, Evaluation & admissibility;
- Delays – Nemesis of Electronic Evidence;
- Jurisdiction & enforcement;
- New Domain – new challenges;



# Definition of Document - Dynamism Displayed

- **S.29 IPC & S.3 IEA:** The Word document denotes any matter, expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter”

# Document – Definition Contd.,

- Explanation to S.29 IPC:
  - It is **immaterial** by what means and upon what substance the letters, figures or marks are formed, or whether the evidence is intended for, or may be used in, a Court of Justice, or not.
- S.29A IPC: Electronic Record:
  - The Words “Electronic Record” shall have the meaning assigned to them in Cl. 2 (1)(t) of the IT Act, 2000

# Definitions – IT Act

- **Sections 2(1)**
- **(O): Data**
- **(r): “Electronic Form”**
- **(t): Electronic Record;**
- **(p): Digital Signature;**
- **(ta): Electronic Signature;**
- **S. 79A – Notified Examiner of Electronic Evidence**

# Electronic Evidence – The Great Indian Quagmire!

- S.65B:
- Admissibility of Electronic Evidence;
- All subsections need to be satisfied – impracticability?
- Where lies the solution?
- Looking beyond the obvious:
- S. 62 onwards:
- Standard rules of Evidence would apply *pari passu*

# Admissibility – Electronic Records

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

# Admissibility - Conditional

- (2) Conditions:—
- (a) computer output **produced** by the computer during regular use for storing or processing information in regular usage by person having lawful control over use of the computer;
- (b) during the said period, information regularly fed into the computer in the ordinary course of the said activities;
- (c) during this period, computer was operating properly & during period of disuse, problem was not such as to affect the electronic record or the accuracy of its contents; **and**
- (d) the information fed into the computer in the ordinary course of business activities;

# Admissibility Conditions – still on track

- (3) storing or processing information was regularly carried on over relevant period, through one of the following processes:
  - (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,
- Where multiple computers are used all of them shall be treated as ONE computer;

# Here comes trouble

- (4) Where statement in evidence pertaining to electronic record is to be given, a certificate doing any of the following things:
- (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.



# Some more proving of Electronic Records

- (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 therefrom by calculation, comparison or any other process.

# State of Punjab v. M/s. Amritsar Beverages Ltd (SC; 08.08.2006)

- Creative interpretation to be resorted to by Court to achieve balance between age old and rigid laws on the one hand and the advanced technology, on the other – with respect to copying & retention of data in soft form (Punjab General Sales Tax Act, 1948);
- Internet and other information technologies brought with them issues not foreseen by law as for example, problems in determining statutory liabilities.
- It also did not foresee difficulties faced by officers without scientific expertise or without sufficient insight to tackle the new situation.
- Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus.
- Information Technology Act, 2000 although amended to include various kinds of cyber crimes and the punishments there for, does not deal with all problems which are faced by the officers enforcing the said Act.

# State v Mohd. Afzal & Ors (Delhi High Court - 2003)

- Parliament attack case - IMEI Nos & laptop seized relied upon;
- S.65B permits proof by Secondary evidence when original is of such a nature as not to be easily movable. Computerised operating systems and support systems in industry fall within this category;
- Electronic record produced there from has to be taken in the form of a print out, which is admissible without further proof, subject to satisfaction of the conditions mentioned in S.65B. Sub-section (4) provides an alternative method to prove electronic record and not the ONLY method to prove electronic record." (Emphasis supplied);

# State v Navjot Sandhu @ Afsan Guru (SC; 04.08.2005)

- Parliament Attack case – confirmation of sentence by Supreme Court;
- S.63 & S.65 IEA: Admissibility of Electronic Evidence; interpretation of S.65B reinstated – proving as Secondary evidence (printouts taken by mechanical process & certified by a responsible official held sufficient in the absence of Certificate under S.65B (4));
- Conviction upheld *inter alia* on evidence pertaining to IMEI nos & materials on laptop seized;

# Reversal of Fortunes – Navjot Sandhu Overruled!

- Anvar PV. Vs PK. Basheer and others (SC):  
(2014):
  - Compliance with entire provision of S.65B including sub clause (4) mandatory;
  - Legislative intent clear and cannot be overlooked;
  - Necessity for certificate emphasized;
  - Clarification of pending cases where trial already completed based on Navjot Sandhu not given;
  - Clarification on separate certificate Vs. inherent certificate absent;

# Anvar Interpretation

- S.65B(4):
  - (a) There must be a **certificate** which **identifies** the **electronic record** containing the statement;
  - (b) The certificate must describe the **manner** in which the electronic record was **produced**;
  - (c) The certificate must furnish the particulars of the **device involved in** the **production** of that record;
  - (d) The certificate must deal with the applicable conditions mentioned under **Section 65B(2)** of the Evidence Act; and
  - (e) The certificate must be **signed by** a **person occupying** a **responsible official position** in relation to the **operation of the relevant device**.
- Certificate to the best of deponent's knowledge and belief.
- Certificate to accompany the electronic record, when the same is produced in evidence.

# Reading in S.65B(2)

- Section 65B(2) of the Evidence Act:
  - (i) The electronic record containing the information should have been produced by the computer during the period over which the same was regularly used to store or process information for the purpose of any activity regularly carried on over that period by the person having lawful control over the use of that computer;
  - (ii) The information of the kind contained in electronic record or of the kind from which the information is derived was regularly fed into the computer in the ordinary course of the said activity;
  - (iii) During the material part of the said period, the computer was operating properly and that even if it was not operating properly for some time, the break or breaks had not affected either the record or the accuracy of its contents; and
  - (iv) The information contained in the record should be a reproduction or derivation from the information fed into the computer in the ordinary course of the said activity.

# Gajraj vs State (Delhi High Court – 18.05.2006)

- Investigation of a murder through tracing IMEI number (International Mobile Equipment Identity) and Accused convicted;
- Conviction upheld in appeal;
- Questions of appreciation of electronic evidence raised qua IMEI no;
- Relied on Mohd Afzal & Navjot Sandhu case supra;



# Tape Recording & Electronic Evidence

- Dilip K. Bandopadhyay Vs. State (Delhi HC – 2013): Reliance on Tape recorded messages upon proof of:
  - Relevance of conversation;
  - identification of voice;
  - Accuracy of the tape-recorded conversation by eliminating possibility of erasures;
- Argued as electronic record u/s.65B;
- Reiteration of mandatory compliance of S.65B conditions;

# Dharambir Vs. CBI (Delhi HC) – 11.03.2008

- S.207 Cr.P.C & Electronic Records:
- Four cases of recorded telephone conversations (through wire tapping);
- Analysis of Sections 173 (5) and 207 of the Code of Criminal Procedure 1973 (CrPC), Sections 3 and 65B of the Indian Evidence Act 1872 (“EA”) and Sections 2 (o) read with Section 2 (t) of the Information Technology Act, 2000 (IT Act);
- Bribery Case – School Case (Building Constructions violations etc.,)

## Dharambir – Contd.,

- Transcripts of relevant portions of the conversation and CD furnished to Accused;
- Accused filed Applications for Mirror Images of recordings to be provided;
- Special Judge CBI refused such request;
- WP under Articles 226 & S.482 Cr. P. C filed before Delhi High Court;

# Dharambir – Court's Decision

- Conversations recorded in those hard discs were certainly „documents“ within the meaning of Section 3 EA read with Section 173 (5)(a) and 207 (v) CrPC;
- "Evidence".-"Evidence" means and includes (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; Such statements are called oral evidence;
- (2) [all documents including electronic records produced for the inspection of the Court]; such documents are called documentary evidence.”

# Appreciation of Electronic Evidence

- A hard disc that is once written upon or subjected to any change is itself an electronic record even if does not at present contain any accessible information;
- A reading of Sections 173 (5) (a) and Section 207 (v) CrPC indicates that there is very little discretion left with the court to substitute its opinion as to what the prosecution should be relying upon for proving its case.

# Ujjal Dasgupta vs State on 25.04.2008

- Accused illegally procured certain classified documents from his office at the National Security Council Secretariat for being supplied to foreign agents;
- Electronic Evidence on pen drives & hard discs
- Takes Dharambir forward for furnishing copies of hard copies of electronic documents to be furnished to Accused;

# Ram Alias Ramprasad Vs. State (Madras High Court - 2014)

- Videograph & CD seized are Electronic Records;
- Distinguished from Article;
- Necessity to furnish copies of such electronic records emphasized & ordered;
- Trial Court directed to furnish copies;
- Non – furnishing would amount to denial of opportunity to the accused in the trial (173 & 207 Cr. P.C);

# Best Evidence – Electronic Evidence

- **Tomaso Bruno Vs. State of UP: (SC) 2015:**
- With the advancement of information technology, scientific temper in the individual and at the institutional level is to pervade the methods of investigation.
- With the increasing impact of technology in everyday life and as a result, the production of electronic evidence in cases has become relevant to establish the guilt of the accused or the liability of the defendant.
- Electronic documents *strictu sensu* are admitted as material evidence.
- non-collection of CCTV footage, incomplete site plan, non-inclusion of all records and sim details of mobile phones seized from the accused amount to withholding of best evidence;
- Offence U/s.302 IPC – prosecution errors resulted in acquittal;



# Other relevant Provisions

67A

- Proof as to digital signature

73A

- Proof as to verification of digital signature

81A

- Presumption as to Gazettes in electronic forms

85A

- Presumption as to electronic agreements

85B

- Presumption as to electronic records and digital signatures

# Other relevant Provisions

85C

- Presumption as to Digital Signature Certificates

88A

- Presumption as to electronic messages

90A

- Presumption as to electronic records five years old

131

- Production of documents or electronic records which another person, having possession, could refuse to produce

# Who Exactly is an Expert?

- Has the scope of the definition been restricted because of new additions?
- S.45: Expert Evidence: Broad definition; Purposive interpretation to read in Cyber Forensics?
- S.45A: Opinion of the examiner of electronic evidence (as in S. 79A of IT Act) is relevant fact;
  - Explanation: For the purposes of this section, an Examiner of Electronic Evidence shall be an expert;S.45A: Opinion of Examiner of Electronic Evidence:
  - Applicable only to the Central or State Government Authority appointed under S.79A of IT Act is deemed to be an Expert for Cyber Forensics!!!

# More on Experts for Electronic Evidence

- S.47A: Opinion of Certifying Authority issuing digital signature is a relevant fact, for Court to form an opinion on the digital signature of any person;
- **S.79A: EXAMINER OF ELECTRONIC EVIDENCE:**
  - Department, body or agency of the Central Government or a State Government notified by Central Government as Examiner of Electronic Evidence to give expert opinion on electronic form evidence before any court or other authority;
- Restrictive and not inclusive definition;
- Overreach of legislators? Or oversight?
- Where lies the remedy?

# Proving the impossible?

- Difficulty in establishing beyond reasonable doubt;
- Technologies for hacking; cloning; faking & more;
- It was not I – an airtight defense?
- Reliance on offline correlations – our best bet!
- Delays & electronic evidence – true enemies!

# First Principles & Last Words

- Access:
  - retaining & ensuring authenticity & integrity;
  - Protect against tampering / loss of data;
  - Handling of storage mediums;
- Preservation:
  - Chain of Custody;
  - Retention of virtual trail for authentication & proof;
  - Retention of paperwork with author details for proving documents;
  - Ensuring eligibility criteria of authors / experts / investigative agencies;
  - Adherence to collation procedures including independent and knowledgeable witnesses;

# Defining Jurisdiction

- **Jurisdiction:** A Court's power to decide a case or issue a decree; A Geographical area within which political or judicial authority may be exercised (Black's Law Dictionary);
- It is the settled position in law that jurisdiction of courts comes solely from the law of the land and cannot be exercised otherwise. (***A.R. Antulay v. R.S. Nayak, (1988) SC***);

# Jurisdiction - Essentials

- (1) A court created by law, organized and sitting;
- (2) Authority given to it by law to hear and determine;
- (3) Power given to it by law to render a judgment;
- (4) Authority over parties to the proceedings – submission to jurisdiction or exercise thereof;



# Jurisdictional Nemesis

- **Civil:**

- Casio India Co. Ltd v. Ashita Tele Systems Pvt. Ltd (2003);
- (India TV) Independent News Vs. India Broadcast Live LLC (2007) (Del);
- Banyan Tree Holding Vs. A. Murali Krishna Reddy (2008):
  - Basis for jurisdiction in online transactions:
    - Purposive availment;
    - Minimum Contacts
    - Interactive Websites alone insufficient;

# Jurisdiction

- Criminal:
- S.4 IPC: offences affecting computers;
- S.179 Cr.P.C: Acts & Consequences vesting jurisdiction;
- S.188 Cr.P.C: Citizens anywhere & Non Citizens on Ships & Aircrafts registered in India;
- S.75 IT Act: Extra territorial jurisdiction for any offence affecting computer, computer resource or computer network in India;

# IPC on Extra Territorial Jurisdiction

- S.4:Provisions of Code apply to any offence committed by—
  - Any citizen of India in any place without and beyond India;
  - Any person on ship or aircraft registered in India where ever it may be;
  - Any person in any place without and beyond India committing offence targeting a computer resource located in India;
  - Offence: act committed outside India, which would be punishable under Code if committed in India;

# Long Arm under Cr. P.C

- **S.179 Cr. P. C:** Act an offence because of anything done **and** consequence which ensued, then Court where either the Act was done or where the Consequence ensued will have jurisdiction;
- **S.188 Cr.P.C:** Offences committed outside India:
  - by citizens on high seas or elsewhere;
  - by non citizens on ship or aircraft regd., in India;
  - May be dealt with as if such offence had been committed within India;
  - Trial at place where offender is found;
  - Proviso: **Prior Sanction of Central Government mandatory to try such offences;**

# Extra Territorial Jurisdiction under IT Act

- **S.75:**
  - 75(1): Provisions of Act to apply to offences committed outside India, irrespective of nationality of offender;
  - 75(2): IF act or conduct constituting offence or contravention INVOLVES a computer, computer system or computer network located in India.

# Domain decides the Forum

- Two aspects of jurisdiction for cyber crimes:
  - Domestic offences – Make & break in India!;
  - Cross Border offences – Everything including crimes have gone international;
- Minimum Contacts & Criminal Law:
  - First Principles for all offences & jurisdiction – Cr. P.C;
  - International – rationalizing Cr. P.C & IT Act;

# Jurisdiction Hazards

- Remedy & Rights
- How easy is it to enforce a right?
- Case Study:
  - Complainant – Company dealing with foreign Embassies and Consulates.
  - Case of online defamation by NRI offender on Website & Server in USA;
  - Summons issued by Criminal Court – service through Letters Rogatory;
  - Delays do defeat justice!

# Issues & Concerns – International Cyber Crimes

- Provisions of S.188 Cr.P.C substantially extended;
- Prior sanction however dispensed with for IT Act offences;
- Impact on Cyber Crimes, which transcend one enactment?
- IT Act Vs. IPC? Duality of compliance;
- Cr. P.C to always be read in conjunction with IT Act;
- Implications?
  - Personal jurisdiction extended without voluntary submission;
  - Ignorance of law no excuse including of extra territorial applicability?
  - Extra territoriality read with Vicarious liability – further cause for concern?



# Interplay of Cr.P.C & IT Act

- S.179 Cr.P.C: Citizens & Non – Citizens;
- S.188 Cr.P.C: Citizens everywhere; Non – Citizens on ships & aircraft registered in India; Need for Prior Sanction;
- S.75 IT Act: Citizens & non – citizens;
- Registration of case under IPC & IT – which one takes the cake?

# Letters Rogatory or Purgatory?

- S.166A Cr.P.C: Letters Rogatory – only to Countries with MLATs /MOUs / Arrangement exists / on basis of reciprocity.
- Prior concurrence of Ministry of Home Affairs by Investigating Agency before a request for Letters Rogatory is filed before a Court;
- LR request by private party – Ministry of Home Affairs – with 12 clear weeks from date of receipt;

# Jurisdiction & Enforcement

- Maxwell on the Interpretation of Statutes, has set out, as under:
- *'Where an Act confers a jurisdiction, it impliedly also grants the power of doing all such acts, or employing such means, as are essentially necessary to its execution.'*



**THANK YOU**

**N S NAPPINAI  
ADVOCATE**

nappinai@nappinai.com, nappinai@gmail.com  
# +91-22 - 66330545; +91-22-66352604;