Foundation of
Data Protection Professionals
in India

Evidentiary Challenges in Cyber Forensics

By

Naavi

Foundation of Data Protection Professionals in India

What is Cyber Forensics?

- The Art and Science of
  - Identifying,
  - Discovering,
  - Collecting,
  - Preserving, and
  - Presenting evidence in electronic form
    - Ability to be able to get the discovered evidence admitted in a judicial process is central to the Cyber Forensics Activity

The Challenges in the Privacy and Data Protection context

- When a forensic specialist is excavating evidence, he may accidentally trample on PII.
  - and has to **assume responsibility for Data Protection**
- Evidence requires to be **recognized**
    - even when it is only a “Potential Evidence” and
- Potential evidence has to be **archived**
    - Subsequently, it may have to be **discarded if not required** or **presented** to the appropriate law enforcement/judicial authority
    - The entire process has to be as required under the evidentiary law of the land
- Evidence has to be produced with Section 65B (IEA) certification

When do we invoke a Forensic investigation?

- Forensic Investigation may be necessary
  - When the DPA has raised a data breach query
  - A Data Subject files a complaint that his Right has been infringed
  - The DPO/Auditor suspects a potential data breach recognizing that an “incident” indicates a “Harm” to a data subject
- Before a “Data Breach” is announced, the forensic audit is required to assess
  - Whether a data breach has really occurred
  - If so what has been breached? And what “Harm” has been caused to the Data Principal/Data Subject
    - Who is accountable etc..comes in the next stage

Rights of the appointed Investigator

- The Forensic investigator may be an employee or an outside consultant
  - He may not be one of the authorized persons to access the PII.
  - **A Contract** has to be issued which provides the access and pinning the investigator to certain responsibilities
    - That he will exercise all due care not to damage the data or
    - That he will exercise all due care not to cause the data to be exfiltrated
    - That he will keep complete evidence of all his activities
    - That he will produce a Section 65B certified evidentiary report
      - May be required even for the internal auditor

Rights of a Investigator by force of law

- Is determined under law based on the status of the person as a “Law Enforcement Official”
  - It is however necessary to examine if the law Enforcement authority itself is bringing in an external consultant as an expert with his own tools/computer and there is a likelihood of evidence getting transferred to the investigator

Rights of a legally empowered Investigator

- Under ITA 2000/8
  - Rights are exercised by an Adjudicator (Sec 46) or
  - A Police officer not below the rank of an Inspector (Sec 78)
  - Official of the Government authorized under Section 69 (Interception),69A (Blocking),69B (Traffic Data),70B (CERT-IN) of ITA 2000/8
  - Through a Court under
- Before granting access, precautions are required to be taken to ensure that the right person under the right authority is exercising the authority
  - Any excess may be an offence under Section 72 of the Act and punishable under Section 66

Rights of a legally empowered Investigator

- Under PDPA 2018, apart from the DPA
  - Police Inspector (Sec 94)
  - Officials exercising the powers under Section 43
    - Processing of PD in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law as authorized by law
      - Could be under IPC or IEA or any other act
    - Or a Court
      - Need to ensure that the authority is properly exercised

Rights of an Insurance Investigator

- In case of Cyber Insurance
  - The Insurance investigator may seek permission to conduct a forensic audit of his own.
    - Basis is the Insurance Contract
    - Must be accountable to Indian laws

Rights of the External Investigators

- Under GDPR
  - The supervisory authority is an outsider and may not have jurisdiction
  - All rights are through contract
  - But the local company cannot grant rights contrary to what is available in the Indian law
    - Preferred method is to let the investigation happen under the local company only which can share its findings as required with the upstream data controller/processor

Rights of an External Investigator

- Any data accessed for investigation
  - Must be purpose specific and
  - Must be destroyed after the authority ceases to exist.
    - Must be documented in the letter of authority

What is Potential Evidence

- Something which is not an evidence today but could be considered so tomorrow.
  - A subjective opinion is required
  - Requires understanding of the Techno Legal impact of incidents with an appreciation of the applicable law
  - Company should enable intervention of appropriate senior persons to flag the incidents through its “Data Disclosure Policy”
  - Once an electronic document is declared as “Potential Evidence”, it has to be securely achieved until its status either changes to “Evidence” or cleared for being reverted out of the “Potential Evidence” status

Section 65B Certification

- Section 65B of IEA enables consideration of Certified “Computer Output” as admissible evidence
  - “without production of original”.
- When a law enforcement officer comes in search of evidence,
  - Section 65B enables the company to provide only the relevant electronic document so that there is no need for “Seizure” of hard disk or CD or other unrelated evidence

Section 65B Certification

- Under Section 65B,
  - The electronic document that is required for evidence is reproduced either as a print out or an electronic copy and would be accompanied by
    - Details of the manner in which they were accessed for the purpose of the report
    - Details of the person who observed the documents, captured them, converted them into “Computer outputs” and his signature
    - Details of the devices used (hardware and software) and the manner of their usage
    - A few warranties such as the computer producing the computer output was working properly,..etc as provided in Section 65B(4)

Section 65B Certification

- Section 65B Certificate is mandatory for any electronic document to be admitted as evidence.
- In the case of Forensic investigations where the evidence is “Discovered”, it is important for the investigator to record the forensic methodology used along with the devices before certifying the end electronic documents.
- The description of process should be reasonable enough for a person with similar expertise to repeat the process in which case he is expected to derive the same results, other things being equal.

Section 65B Certification

- In many cases, the “Document at the Source” from which the “Section 65B certifier” extracted and observed the document on his device and produced the computer output
  - Might have later been erased.
  - In such cases the Computer output will be the only copy of the evidence that would be available.
    - Hence the credibility of the provider of Section 65B certificate is very critical to the Court in accepting the evidence without qualification

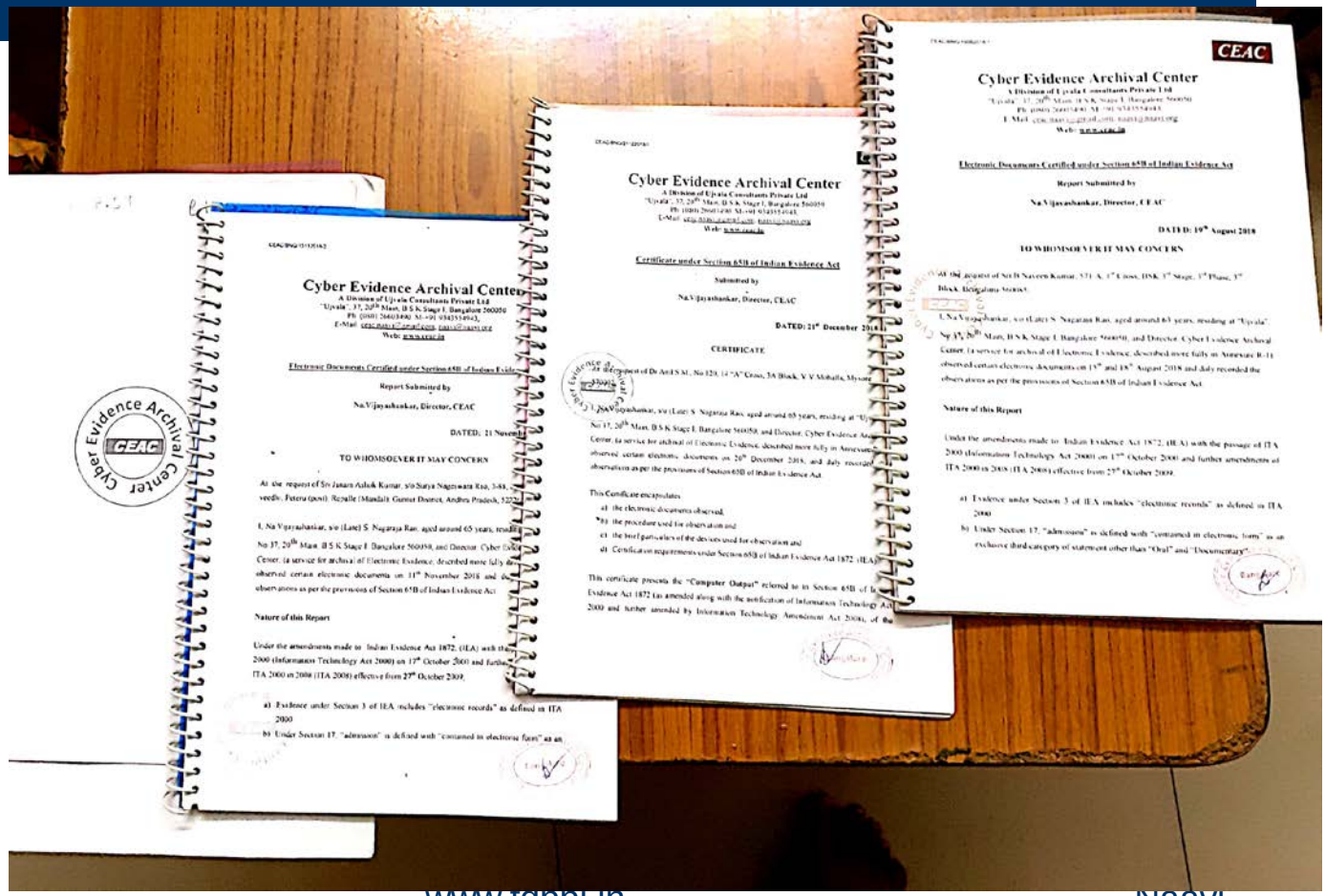
Section 65B Certification

- Section 65B certified Computer output is admissible as evidence without the production of the original
  - However once admitted, the counter party can challenge the “Genuinitity” of the evidence by producing its own counter evidence.
  - If the Court requires confirmation on its own, then it can call in the services of a Section 79A (ITA2000/8) accredited “Digital Evidence Examiner”.

Section 65B Certification

- In certain instances electronic evidence may be transferred from one source container to another over a period
- Final certificate may be from one such “Container of Electronic Document” (Example: CD or Memory Card)
  - In such cases, Sec 65B certificates are required for each transfer of the document from one device to another.
    - Contemporaneous certificates

CEAC Certificate is more than a stamped image



Section 65B Certification

- For more clarity, visit www.ceac.in
- Check the Supreme Court judgement in the case of P V Anvar Vs P K Basheer
- See E Book titled “Section 65B of Indian Evidence Act Clarified” available at www.naavi.org

Summary

- Success of Cyber Forensics does not end with undeleting the deleted files or viewing hidden log records, but
  - Extends to producing certified copies admissible to a juristic authority.
  - The DPO who is in most cases supervising the audits of suspected data breaches etc has the responsibility to appreciate the procedural requirements of Section 65B to ensure that the process is acceptable under law

Questions

- Naavi
  - www.naavi.org
  - www.ceac.in
  - www.fdppi.in
  - naavi@naavi.org
  - 9343554943