EVALUATION OF ELECTRONICALLY GENERTAED EVIDENCE PRACTICE AND PROCEDURE

Shafiu R. Mahmud

Federal Ministry of Justice.

INTRODUCTION

AIMS AND OBJECTIVES

- The aim of the presentation is tailored to acquaint the participants who are triers of fact on evaluation of electron evidence (e-evidence) and practice and procedure.
- At the end of the session the participant are expected to know what to bear in mind when evaluating e-evidence presented before them.

INTRODUCTION

- Prior to the amendment of Evidence Act 2004, the pursuit of justice seems to be very tedious, frustrating and sometimes without success especially when the evidence involved are digital evidence or electronic evidence nature.
- However with coming of Evidence Act 2011 it makes easier for the presenter of the e-evidence to present the evidence before the court if the said presenter satisfy the condition laid down in S.84 of the Act. [1]

WHAT IS EVIDENCE

- It simply refers to piece of information or thing put before a court in order to prove or disprove facts in issue. [1]
- Traditionally and historically, evidence has been in a physical form (such as documents or photographs etc.) or the oral testimony of witnesses.

- 1. Electronic Evidence (Revise Edition) A.O. Ajileye

ELECTRONIC EVIDENCE

- Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet.
- Note: Evidence Act 2011 does not define what e-evidence means, however, s.258(1) defines what computer means.

SOURCES OF E-EVIDENCE

CHARISTERISTICS OF E-EVIDENCE

- **It is invisible to the untrained eye**: e-evidence is often found in places where only specialists would search or in locations reachable only by means of special tools.
- **It is highly volatile**: is highly fragile and easily lost or altered if appropriate precautions are not followed
- **It may be altered or destroyed through normal use**: Computer devices constantly change the state of their memories, be it on user request or automatically by the computer operating system
- **It can be copied without degradation**: Digital information can be copied indefinitely with each copy exactly the same as the original.

EVALUATION OF ELECTRONIC EVIDENCE

EVALUATION OF E-EVIDENCE

- **NWABUOKU V ONWORDI (2006) 26 NSCQR, 1161 @ 1165**
- "It is not the law that every document admitted by a court of law must be assigned probative value. A document could be admitted on the ground of relevancy **but the court may not attach any weight on it** in the light of the circumstance of the case. In other words, admissibility which is based on relevancy is distinct from weight to be attached to the document".

EVALUATION OF E-EVIDENCE

- A document that has been electronically stored or generated may be admissible in court but a judge may attach little or no weight to it.
- S.34 (1) EA provides guidelines in estimating weight to be attached to a document produced by a computer

EVALUATION OF E-EVIDENCE

Points To Be Derive From s.34 of EA

- Circumstances from which any **inference** can reasonably drawn as to the accuracy or otherwise of the document or data

- Consideration as to whether or not the information reproduced from the computer was supplied or recorded contemporaneously with the existence or occurrence of the fact dealt with in that information

- Whether or not the person concern with the supply of the information to the computer has incentive or motive to conceal or misrepresent the information so supplied.

EVALUATION OF E-EVIDENCE

Examples From Other Jurisdictions

- In the Indian Case: State of Delhi v Mohd Afzad & Ors. (2003)DLT 385. it was held that if someone challenge the accuracy of a computer or electronic-evidence on the ground of misuse or operating failure, he must prove same beyond a reasonable doubt.
- The court observed that mere theoretical or general apprehensions cannot make clear evidence defective and inadmissible.

CONCLUSION

- It very important for judge or magistrate when handling cybercrime cases or a case where parties relies so much on electronic evidence to know the type of witness before him.
- Basically there are two types of witness
  - Fact Witness
  - Expert Witness

CONCLUSION

FACT WITNESS

- Is testify about what he did, what processes he undertook and/or how he got from Point A to Point B
- A Fact witness can only testify to a fact which was actually undertaken or observed by one of the 5 senses
- Unless testifying as an expert, you can only testify to what you personally saw, heard, or did
- No speculation, No hearsay.

CONCLUSION

EXPERT WITNESS

- An Expert witness posses a scientific, technical or specialized knowledge, training, skill or experience which will assist the judge to understand the evidence or to determine a fact in issue.
- An expert witness may testify in the form of an opinion

- **THANK YOU**