KTA ADVOCATES

AMANI IP NETWORK

Kampala | Dar es Salaam | Nairobi

ELECTRONIC EVIDENCE

LEGAL ALERT

INNOVATE · GROW · DISCOVER

Our Core Purposes

We Exist To Offer Innovative Service That Nurtures Relationships And Impacts Lives

Preface

Covid – 19 after effects present an opportunity for technology to grow beyond expected projections; businesses have now translated to Internet based models as part of the new normal which makes use of the internet inevitable. With transactions conducted over the internet, courts and litigants must be prepared to use electronic evidence as part of their case strategy. Uganda has enacted relatively sufficient legislation to fully enable the use of digital evidence as noted in the text.

Internet penetration in the region has since increased. The most recent survey done by Internet World Stats reveals that Uganda ranks 15th in Internet usage across Africa with Kenya leading the pack. The growth of internet usage despite its high cost is visible; in 2000, the penetration percentage was 0.1 % and in 2016, the percentage was 31.1 % that is 11,924,927 million people out of 38,319,241 people in Uganda, with Kenya having 77.8% penetration. With transactions made over the internet, the modern Bar and Bench must equip themselves with enough knowledge on electronic evidence and its admissibility in courts of law.

The paper is therefore timely in Uganda as courts are determining cases departing from the traditional rules of evidence. The paper addresses authorities both from statutes and decided cases on the subject with additional authorities from other jurisdictions.

"Uganda's Evidence Act was passed long before the computers were invented and the issue of electronic evidence could not have been contemplated, it is important that Uganda moves forward into the digital age in a way that makes it possible to resolve legal disputes effectively" commodity Export International Limited versus NKM Trading Company Limited CACA 84 of 2008.

Introduction

Evidence plays an important role in the administration of justice. It helps to guide legal proceedings by determining the type of facts that can be admissible as evidence. The Evidence Act of Uganda is cited as the Evidence Act, Cap 6. It was enacted in 1909[1] and has not undergone major reform despite numerous developments in the area of evidence law, including technological developments and the changing nature of information.[2]

The Evidence Act, Cap. 6, like most of Uganda's legislation was received from the British and commenced on 1st August, 1909. The Act was derived from the Indian Evidence Act of 1872 which was an attempt at codification of English Common Law. Uganda was a protectorate under the British Government from 1894 to 9th October 1962. The Act was implanted in Uganda with little regard to the social, economic and cultural conditions.

The paper re-visits the traditional rules of evidence law as developed overtime and reveals the shift that has occurred with respect to electronic evidence especially on the exception of hearsay and that of primary evidence. The paper looks at the earlier position of law in this regard and subsequent changes, the amendments to law, and a few possible effects of such amendment.

The present law on evidence in Uganda recognizes the 'Best Evidence Rule' requires that only original documents in a written form can be admissible in courts of law, in case of dispute, the admissibility and weight of this kind of evidence can be a challenge.

Due to the advancement of digital technology, the use and scope of electronic evidence has expanded greatly all over the world. While many Ugandans having adopted the use of technology, reliance on the 'Best Evidence Rule' as provided under the Evidence Act can pose challenges for admissibility of electronic evidence.

In addition, Uganda enacted three laws relating to electronic evidence namely:

a) The Computer Misuse Act, No. 2 of 2011;

b) The Electronic Signatures Act, No. 7 of 2011; and

c) The Electronic Transactions Act, No. 8 of 2011;

The Computer Misuse Act provides for *inter alia*, the security of electronic transactions and information systems; prevention of unlawful access, abuse or misuse of information systems and for security of electronic transactions. The Act creates offences for unauthorized use, access, abuse of computers or data. Offences under the Act also include electronic fraud, child pornography, cyber harassment and stalking.

Section 9 (1) of the Computer Misuse Act, 2011 provides for a preservation order where an investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system, where there are reasonable grounds to believe that such data is vulnerable to loss or modification. This is an exparte order and the determination of this application should be expeditious so that the evidence is not destroyed.

The Electronic Transactions Act provides for the use, security, facilitation and regulation of electronic communications and transactions as forms of communication. The Act provides

1 Commenced on 1st August 1909

2 Vastina Rukimirana Nsaza presentation By Uganda Law Reform Commission on the Law of Evidence ALRAESA conference on 29th – 30th June, 2017.

legal certainty in respect of validity, legal effect and enforceability of information in electronic form; it relates electronic evidence to electronic transactions but does not give the use of electronic evidence general application.

The Electronic transactions Act[3] makes electronic evidence admissible in courts, Electronic Signatures Act[4] makes provision for the use of electronic signatures in order to ensure that transactions are carried out in a secure environment, establishes a public key infrastructure for authenticity and security of documents and recognizes the different signature creating technologies.

It should be noted that whereas The Judicature (Visual-Audio Link) Rules, 2016 makes it more affordable to use technology to conduct proceedings in courts of law, these aim to provide for the taking of evidence in court by visual-audio link and to make it easier for witnesses to give evidence without physically appearing in court and their evidence does not constitute electronic evidence. The use Visual-Audio Link is merely an administrative channel for expeditious determination of disputes and does not constitute electronic evidence.

The Constitution (Integration of ICT into the Adjudication process for courts of Judicature) (Practice Directions), 2019 provides for electronic service of court documents, providing for electronic versions of documents including pleadings, emphasizing use of technology.

What is electronic evidence

Defining electronic evidence may be problematic especially with advanced technology for example with Artificial Intelligence it will be very hard to examine robots on their actions. But different scholars have struggled to come up with a universal definition of electronic evidence.

George and Stephen Mason define Electronic evidence as all **information with probative value** that is included in an electronic media or is transmitted by media.[5] George and Stephen give an expansive definition as data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication.

Justice Mutonyi in the case of *Amongin Jane Francis Okili Vesus Lucy Akello and The Electoral Commission*[6] has defined electronic evidence as is any probative information stored or transmitted in digital form that a party at a trial or proceeding may use. It is used to prove a particular proposition or to persuade court of the truth of an allegation.

In his treatise, Casey defines digital evidence as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offence.[7] Although Eoghan's definition is in criminal investigations, it is wider than the previous definitions, and it usefully explicates certain important aspects of electronic evidence.

3 Act Number 4 of 2011 commenced 18th March, 2011. Accessible at https://ulii.org/ug/legislation/act/2015/8-3

4 Act Number 7 of 2011 Accessible on https://www.nita.go.ug/publication/electronic-signatures-act-2011-act-no-7-2011

5 Electronic Evidence, George, Madson University of London Press, Institute of Advanced Legal Studies, 2017. Accessible via https://www.jstor.org/stable/j.ctv512x65

6 HCT-02-cv.0001 – 2014 Accessible at https://ulii.org/ug/judgment/election-petitions/2015/1 (last accessed on 25th April, 2020.

7 Eoghan Casey, Digital Evidence on Computer crime 3rd Edition Academic Press, 2011

For instance, the reference to 'data' is to information that is held in electronic form, such as text, images, audio and video files. Also, the word 'computer' must be understood in its widest possible sense, and incorporates any device that stores, manipulates or transmits data.

From the above, the universal accepted definition of Electronic evidence is data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.

For this, we distinguish **two basic types of electronic evidence:**

1. Data stored in computer systems or devices.

2. Information transmitted electronically through communication networks.

Various devices are capable of creating and storing data in digital form, and such data may serve as evidence, this includes data that is input or created in the computer, information transmitted is one communicated through a media device through a network or direct transfer.

Authentication

Electronic documents are easy to manipulate and they can be copied[8], altered, updated, or deleted (and deleted in the electronic environment does not mean expunged). The integration of telecommunications and computers to form computer networks (such as wide area networks and the Internet) further allows data to be created and exchanged in far greater volumes than had hitherto been possible, and across physical and geographical boundaries. In essence, email, instant messaging and Internet communications are a duplicate and distributed technology.[9]once computers are networked together in this fashion, an electronic document may be transmitted and different copies may be distributed and altered to various people instantly.

8 Allegations in Vestergaard Frandsen A/S v Bestnet Europe Limited [2007] EWHC 2455 (Ch), which is a judgment in relation to an application by the defendants to strike out the action on the grounds that it was vexatious and an abuse of the process; George L Paul and Jason R Baron, 'Information inflation: can the legal system adapt?' (2007) 13 Rich J L & Tech 1.

9 Social media websites and sending text messages on mobile telephones and other devices were used to foment rioting in the UK in 2011: R v Blackshaw and others [2011] EWCA Crim 2312.

Courts in Uganda have established that for electronic evidence to be admissible it must be authenticated. Digital evidence is often attacked for its authenticity due to the ease with which it can be modified although it would be necessary to sustain such an agreement with proof of tampering.

Authentication defined

To be admitted as evidence, an electronic message must first be authenticated or identified. Authentication is the process by which the authenticity, or genuineness, of the document is established. Whether the document is what it purports to be is a matter of conditional relevance i.e. the document is relevant only if the document is what it purports to be.[10]

The person in charge of the process of acquiring information through the electronic process has the responsibility for ensuring that certain standards are met because this kind of evidence can easily be modified and or duplicated. The danger with such digital evidence is that it can easily be created, tampered with or modified in one way or another. Courts should therefore be very careful before admitting it especially if such evidence is contested.[11]

S.5 of the Uganda Electronic Transactions Act 2011 provides that information shall not be denied legal effect, validity or enforcement solely on the ground that it is wholly or partly in the form of data message.

S.7 (2)(a) provides that *"for the purposes of subsection 1(a) (which talks of the original form) the authenticity of the data message shall be assessed (a) by considering whether the information has remained complete or un altered except for addition of an endorsement and any change which arises in the normal communication."*

S. 8(5) of the Electronic Transactions Act[12] provides ***" the authenticity of the electronic record system in which an electronic records system is recorded or stored shall in the absence of evidence to the contrary be presumed where (a) there is evidence that supports a finding that at all material times, the computer system or other similar device was operating properly or if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds to doubt the integrity of the electronic records system.***

The Act defines data under section 2 (1) to mean electronic representations of information in any form and "data message" to mean data generated, sent, received or stored by computer means a stored record. Under the Act "electronic communication" means a communication by means of data messages and "electronic record" means data which is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device and includes a display, print out or other output of that data.

The legal effect of electronic records under section 5 of the Electronic Transactions Act provides that information shall not be denied legal effect solely on the ground that it is in the form of a data message (i.e. email). The information has to be in a form of in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as the information is reasonably capable of being reduced into electronic form by the party incorporating it. For a written document the requirements of the law are met where the information is accessible in the form of a data message and accessible in a manner which is usable for subsequent reference.

---

10 Dian GF International Ltd Vs Damco Logistics Ltd & Trantrack (CIVIL SUIT NO 161 OF 2010) [2012] Accessible on https://ulii.org/ug/judgment/commercial-court/2012/10 Last accessed on 25th April 2020.

11 Coil Ltd v Attorney General (CIVIL SUIT NO.799 OF 2014) Accessed at https://ulii.org/ug/judgment/commercial-court-uganda/2020/3 (Last accessed 22nd April, 2020)

12 Supra

It follows that before admissibility the document has to meet the requirements of authentication or identification. This is a process of verification that establishes that the document is what it purports to be. I.e. that the email was made by the author indicated therein and is unaltered except for the change in the document generated automatically such as adding the date and time in case of email and address.

As far as admissibility and weight of evidence of electronic data is concerned section 8 of the Electronic Transactions Act 2011 gives the principles thereof and provides that rules of evidence shall not be applied to deny admissibility on the ground that it is merely a data message or electronic record where it is the best evidence that the person adducing the evidence could reasonably be expected to obtain or on the ground that it is not in the original form.

The burden is on the person adducing the data message to prove its authenticity by adducing relevant evidence therefore that the document is what it purports to be. Where best evidence is the evidence required, the rule of best evidence is fulfilled upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored. In assessing the evidential weight the court shall have regard to the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the authenticity of the data message was maintained; the manner in which the originator of the data message or electronic record was identified; and any other relevant factor.

The authenticity of the electronic records system such as a computer is presumed in the absence of any evidence to the contrary where there is evidence that the system was operating properly. Where the record is stored by a party adverse to the production of the email or data message; evidence is led that the record was stored in the usual and ordinary course of business by a party who is not a party to the suit.

A video recording for example has since in law regarded as a document.[13] It has been decided by courts that there is no difference in principle between a tape recording and a photograph.[14] Being a document, like any other document being offered in evidence, a recording must be authenticated, a witness must offer evidence establishing that the object is what that witness claims it is. One frequently cited authentication regime was first articulated by the Georgia Court of Appeals. In *Steve M. Solomon, Jr., Inc. v. Edgar 88 S.E.2d 167 (Ga. Ct. App. 195),* where the court stated:

"A proper foundation for [the use of a mechanical transcription device] must be laid as follows: (1) it must be shown that the mechanical transcription device was capable of taking testimony. (2) It must be shown that the operator of the device was competent to operate the device. (3) The authenticity and correctness of the recording must be established. (4) It must be shown that changes, additions, or deletions have not been made. (5) The manner of preservation of the record must be shown. (6) Speakers must be identified. (7) It must be shown that the testimony elicited was freely and voluntarily made, without any kind of duress."

If a participant in the conversation is available to testify, it suffices for the witness to testify that he or she recalls the conversation, has listened to the recording, and is satisfied that the recording accurately captured what was said. It is thereafter sufficient to show a chain of custody which establishes the reasonable probability that no tampering occurred. Minor infirmities in the chain of custody are insufficient to bar admissibility of a recording, but are relevant as to the weight the court chooses to give to it. This requirement can be met when a witness with knowledge testifies generally about how the equipment was set up, the procedures employed, and the records that were kept documenting the

13 ***(see R v Daye 1908 KB 330 at 340 and Seccombe v Attorney-General 1919 TPD 270, 272, 277278)***

14 *(See R v Senat (1968) 52 Cr. App. Rep 282 and Regina v Maqsud Ali, 1965 [1966] 1 QB 688, [1965] 2 All ER 464)*

process. The evidentiary value of a recording depends in large measure on who said what, but a court's ability to use that information depends upon two qualities of the recording: audibility and intelligibility. Audibility relates to whether the listener is able to hear what is on the recording. Intelligibility relates to whether the listener is able to understand what the conversant said.

The issue courts most often focus on is intelligibility. The ultimate test of audibility and intelligibility is whether the party offering the recording has been able to produce a transcript of the recording which accurately reflects the recording's contents.[15]

For that reason, as required by s. 88 of *The Civil Procedure Act*, since evidence in all courts has to be recorded in English as the official language of courts, if the recording is in any other language the transcript of the recording should be translated into English before it can be received in evidence. In the case of *Twaha Sebbi Olegga versus Alidriga Adinan*[16] the recording in this case was never transcribed. It therefore was not tested for intelligibility and audibility. For the reasons stated above court held that part of the pleadings and evidence relating to the video recording ought to have been disregarded by **the trial court.**

Presumption of computer reliability.

This part considers the common law presumption in the law of England and Wales that *'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time'*.[17]

The aim of the presumption alleviates the need to prove every item of evidence adduced in court, or to reduce the need for evidence in relation to some issues, to save 'the time and expense of proving the obvious'[18]. In an appeal before the Supreme Court of South Australia in the case of *Barker v Fauser*[19] regarding the accuracy of the readings of a weighbridge, Travers J explained the rationale as follows: *It is rather a matter of the application of the ordinary principles of circumstantial evidence. In my opinion such instruments can merely provide prima-facie evidence in the sense indicated by May v. O'Sullivan [(1955) 92 CLR 654].*

They do not transfer any onus of proof to one who disputes them, though they may, and often do, create a case to answer. Circumstantial evidence is something which is largely based upon our ordinary experience of life. ... It is merely an application of this principle to our ordinary experience in life which tells us of the general probability of the substantial correctness of watches, weighbridges and other such instruments.

Conversely, in DPP v McKeown; DPP v Jones1 Lord Hoffmann voiced the opinion in 1997 that *'It is notorious that one needs no expertise in electronics to be able to know whether a computer is working properly'*.[20]

Electronic evidence can be relied on if the party who alleges has inter alia established its authenticity and the opposite party has not produced any proof of tampering. A holding almost on the same line is found in *Uganda vs Sserunkuma &8 Others*[21] where the Court held;"The authenticity and integrity of electronic evidence is not in question until the party suggesting otherwise can produce

15 *(see R v Rampling [1987] Crim LR 823).*

16 *HCCA 0006 of 2013 , Mubiru J. High Court of Uganda at Arua Accessible at https://ulii.org/ug/judgment/hc-civil-division/2016/63 last accessed 1st May 2020.*

17 1 Halsbury's Laws (5th edn, 2015) vol. 12, paras 712–23. 2 Law Commission, Evidence in Criminal Proceedings: Hearsay and Related Topics (Law Com No 245, 1997), para 13.13; for the United States of America, see Coleen M Barger.

18 Holt v Auckland City Council [1980] 2 NZLR 124, per Richardson J at 128.

19 (1962) SASR 176

20 [1997] 1 All ER 737, [1997] 1WLR 295, HL; also note the comment by Harvey J in the New Zealand case of R v Good [2005] DCR 804 at 65

21 HC CR SC 15/2013

evidence to say so."

Computer Unreliability

The problem with a presumption that a computer is deemed to be 'reliable' is that as systems become more complex, it has become progressively more challenging to test software to reflect the way the users will actually use the product.

This is because of the large number of functions that software is required to perform, and the unpredictability of the users. Professor Partridge reiterates the point that 'no significant computer program is completely understood[22]', and goes further by indicating that systems are now so complex that humans are no longer able to deal with the problems.

Therefore if the nature of computer-system complexity really is new and peculiar, a system characteristic that has no parallel in the natural world, then our evolutionary history is unlikely to have equipped us to reason effectively with such systems. Our genetic programs may be totally lacking in mechanisms that can deal effectively with discrete complexity.

For example in the New York case of *Porter v Citibank, N.A*[23], customer used his card, but no money was dispensed but a receipt was printed to that effect. Employees of the bank testified that on average machines were out of balance once or twice a week. From an evidence point of view, the information on the print-out is restricted to a single transaction.

Yet, paradoxically, it is a well-known fact in the industry that software could hardly be said to be 'reliable'. As noted by Steyn J in *Eurodynamic Systems Plc v General Automation Ltd*[24], The expert evidence convincingly showed that it is regarded as acceptable practice to supply computer Programmes (including system software) that contain errors and bugs. The basis of the practice is that, pursuant to his support obligation (free or chargeable as the case may be), the supplier will correct errors and bugs that prevent the product from being properly used.

Laying foundation for electronic evidence

This means that where the source of digital evidence has been established and no tampering has been shown by the opposite party it would be admissible like any other documentary evidence. In the case of Coil Ltd v Attorney General[25] where the *Plaintiff stated the source of the Print out as a website of the Ministry of Finance, Planning and Economic Development known to publish current affairs relating to public debts, grants and guarantees, budget monitoring and tax matters. This was not disputed by any evidence oral or otherwise.* It was court's finding that the figure was outstanding and ought to paid to the Plaintiff.

In regard to admissibility of electronic data messages, section 11 of the Electronic Transactions Act, 2011 provides that a requirement for a signature, statement or document to be notarized, or verified or made under oath is fulfilled if an advanced or secure signature of a person authorized to sign the document attached or associated with the electronic document. This was emphasized in the case of Sematimba Peter Simon and another versus Sekigozi Stephen[26]

Before accepting electronic evidence, a court will determine if the evidence is relevant, whether it is authentic, or hearsay,

22 Derek Partridge, What makes you clever – the puzzle of intelligence (World Scientific 2014) 394 and 407

23 123 Misc.2d 28, 472 N.Y.S.2d 582 (N.Y City civ.Ct. 19884).

24 (1983) QB 2804

25 (CIVIL SUIT NO.799 OF 2014) Accessed at https://ulii.org/ug/judgment/commercial-court-uganda/2020/3 (Last accessed 22nd April, 2020)

26 CACA 0008 of 2016.

or whether a copy is acceptable or the original is required. It is apparent that the use of digital evidence has increased in the past and that is why courts which were hesitant to admit it have now accepted it as one of the best evidence. But like any other evidence the proponent of electronic or digital evidence must lay the proper foundation which makes the evidence reliable. Courts are mainly concerned about reliability of such digital or electronic evidence. The points to be considered while laying foundation were lad in the case of Amongin Jane Francis Okili Vesus Lucy Akello and The Electoral Commission[27]

" The foundation should include the following:

1. Reliability of the equipment used.

2. The manner in which the basic data was initially entered.

3. The measures taken to ensure the accuracy of data as entered.

4. The method of storing the data and precautions taken to prevent loss or alteration.

5. The reliability of the computer programs used to process the data.

6. And the measures taken to verify the accuracy of the program

7. What software was used to preserve digital evidence in its original form and to authenticate it for admissibility?

8. The competence of the person who accessed the original data.

9. This person must be competent to do so and able to give evidence explaining the relevance and implication of what he did.

10. An independent third party should be able to examine the process and achieve the same results."

The best evidence rule requires that a party adduce the best evidence available, which in respect of documentary evidence, means that the original of a writing be offered into evidence. When introducing this rule to electronic evidence, it is required if that whether a computer printout is an "original" or "copy". The requirement of originality for paper document is applied differently in email evidence. If data is stored in a computer or similar device, any printout readable by sight, shown to reflect the data accurately, is deemed as "original".[28]

-End-

27 Supra

28 Dian GF International Ltd Vs Damco Logistics Ltd & Trantrack (CIVIL SUIT NO 161 OF 2010) [2012] Accessible on https://ulii.org/ug/judgment/commercial-court/2012/10 Last accessed on 25th April 2020.

TALK TO US

FLoor 3, Plot 4, Hannington Road
P.O. Box 37366 Kampala, Uganda
Tel: 0414 530 114
Fax: 0414 531 078
Email: partners@ktaadvocates.com

WWW.KTAADVOCATES.COM