



Contemporary Issues in Admissibility of Electronically Generated Evidence in Ugandan Courts

CAROLINE ADEKE

School of Law, Victoria University, Kampala, Uganda

cadeke@vu.ac.ug

Abstract. In Uganda, electronically generated evidence arising from a multitude of transactions in the modern contemporary era of technological developments, and constituted in forms of e-receipts, use of e-signatures on transactional documents among others, have created complex difficult situations for admissibility in Court. The paper utilizes the doctrinal research method to examine the effectiveness of the law and practice of evidence in surmounting the recognized challenges the courts face in delivering justice with regards to admissibility of electronically generated evidence in both civil and criminal cases. Analysis is made on how the court admits electronically generated evidence, its authenticity, integrity, and confidentiality in dealing with such evidence. It concludes with recommendations proffered on enhancing admissibility of electronically generated evidence in alignment with the modern contemporary world.

Keywords: Electronically Generated Evidence, Significance, Admissibility, Courts.

1. Introduction

The new normal dictates that electronic evidence becomes part of such evidence used in Ugandan courts. 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 or electronic evidence.¹ Electronically generated evidence is one that is manipulated, stored or communicated by any manufactured device, computer or its system or transmitted in digital form that a party to a trial or proceeding may use.² Usually, electronically generated evidence is used to prove a particular proposition or to persuade court of the truth of an assertion made by the parties to a case. Notably, it is the desire of parties to a suit that their evidence should be admissible, and yet not all evidence brought before the court would be relevant and admissible.³ However, discretion lies on the judge, based on the principles of law, to decide which of the evidence adduced in court is relevant and admissible⁴. Such electronic evidence includes data stored in computer systems or devices and information transmitted electronically through communication networks such as videos, audio messages, text messages, pictures, etc.⁵

¹ Examples include: the Computer Misuse Act, Cap. 96; the Electronic Signatures Act, Cap. 98; the Electronic Transactions Act, Cap. 99; The Judicature (Visual-Audio Link) Rules, 2016; and The Constitution (Integration of ICT into the Adjudication process for courts of Judicature) (Practice Directions), 2019.

² See. Decision by Justice Mutonyi in the case of Amongin Jane Francis Okili Versus Lucy Akello and The Electoral Commission HCT-02-cv.0001 – 2014 Accessible at <https://ulii.org/ug/judgment/election-petitions/2015/1>. Accessed on 20th August, 2025.

³ The best evidence rule has to be prioritized as per the Evidence Act Cap. 8.

⁴ Uvietobore Emuveyan Enaya, Admissibility Of Electronically Generated Evidence in Nigeria, Matric No: 090601120. <https://www.scribd.com/document/722813197/i-ADMISSIBILITY-OF-ELECTRONICALLY-GENERA> Accessed 21 July, 2026.

⁵ KTA Advocates, Electronic Evidence, Legal Alert, 2019. <https://www.ktaadvocates.com/wp-content/uploads/2020/10/ELECTRONIC-EVIDENCE-LEGAL-ALERT-KTA.pdf>. Accessed on 28th June, 2026.

2. Unfolding the Legal Authority

In Uganda, the adversarial trial system remains at the hock of admissibility processes of evidence. Unlike the inquisitorial system which allows Judges to play an active role and descend into the arena of conflict, the adversary trial process, limits Judges to the role of unbiased adjudicators⁶. Leaving Judges to hold the scale of justice fairly and not to make a case for either party. Electronic evidence becomes problematic particularly due to the nature of evidence different from traditional types; and the diverse laws enacted to cater for such evidence in Uganda. The laws seem to have only taken up the substantive side leaving the procedural side to the courts. A case in point, is the Evidence Act⁷ that recognizes the 'Best Evidence Rule' and requires only original documents in written form to be admissible in courts of law, making admissibility and weight of electronic evidence a challenge.

The advancement of digital technology, the use and scope of electronic evidence has expanded greatly all over the world and reliance on the 'Best Evidence Rule' as provided under the Evidence Act poses challenges for admissibility of electronic evidence.⁸ As such no aid has been made to the courts when it comes to deciding what electronic evidence is admissible. The increasing use of digital evidence in proceedings offer new opportunities but challenges as well. As an advantage, electronic evidence in form of e-mail, a satellite intercept, or a video may help establish linkage evidence between the defendant or accused and the commission of an act or a crime. CCTV that captures events relevant to proof in cases can now replace witnesses in court. Digital evidence equally provides information on the time, place, and manner of an event to supplement viva voce evidence or live testimony.

Although commonly, digital evidence can also be altered or degraded. In addition, digital evidence can

be divorced from its source; for example, a photograph captures only one perspective of a location at a specific time, and e-mail does not capture the demeanor or tone of voice of the author. With massive usage of electronics, the courts are bound to find challenges when it comes to admitting electronic evidence in trials because mainly, there is no law in place to guide them. Asanwa mentions that "some cases would have been won easily but for proof of electronically generated evidence were lost."⁹

A) Evidence Act Cap.8

Given the historical background, the Evidence Act was enacted in 1909 and it is shocking that it has not undertaken major reforms despite numerous developments in the area of evidence law. In the contemporary world, major technological developments and the changing nature of information is taking place and omitted to be remedied by the Act.¹⁰ The Evidence Act, now Cap. 8, like most of Uganda's legislation was received from the British and commenced on 1st August, 1909¹¹. The Act was imitative from the Indian Evidence Act of 1872 which was only an attempt at codification of English Common Law.

Uganda, being a protectorate under the British Government from 1894 to 9th October 1962, had the implanted with little regard to the social, economic and cultural conditions. The Evidence Act, being the primary law as regards to admissibility of evidence in Uganda, the fact that it recognizes the 'Best Evidence Rule' as that which requires only original documents in a written form to be admitted in courts makes admissibility and weight of electronic evidence a challenge.

Already there is digital technology advancement, the use and scope of electronic evidence based on the 'Best Evidence Rule' has to continually evolve as a form of document¹² that may be relevant to court.

⁶ Ibid.

⁷ Evidence Act Cap. 8

⁸Electronic Evidence, George, Madison University of London Press, Institute of Advanced Legal Studies, 2017. Accessible via <https://www.jstor.org/stable/j.ctv512x65>

⁹ Asanwa, S. Eyiuche et al., Admissibility of Electronically Generated Evidence in Nigeria: A General overview, Law and Social Justice Review, Vol.4, No.1, 2023.

¹⁰Vastina Rukimirana Nsaza, Uganda Law Reform Commission Annual Report on the Law of Evidence.

ALRAESA Conference on 29th – 30th June, 2017. The paper presented by Vastina the Chairperson by then reviewed the challenges of Uganda's adversarial judicial system and proposed specific legal reforms.

¹¹Commencement date is cited as per the Evidence Act Cap 8 of the Laws of Uganda.

¹² S.2 (1) of the Evidence Act Cap.8 defines a document as 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 for the purpose of recording that matter.

Especially if the document is in its original form and can be produced for the inspection of court,¹³ with exceptions laid out under Evidence S. 62 of the Act. These exceptions laid out under S.62 are unrealistic on two grounds. First, the Act states that secondary copies made from or compared with the original are admissible, which is not true when relying on an electronic record which is prone to distortion.

Secondly, the Act also provides for the exception that copies made from the original by mechanical processes which in themselves ensure accuracy of the copy, and copies compared with those copies. This exception may be applicable to electronic record such as emails but may be far from other records like what up communications.

In a recent Uganda case¹⁴ courts among others considered WhatsApp texts as "data messages" or electronic records, and therefore legally satisfy the requirement of being "in writing" under the Contracts Act¹⁵. Nonetheless, courts may face a serious challenge to cope with these technological developments, especially as regards the treatment of electronically generated evidence arising out of contractual obligations. For instance, sections 91 and 92 Evidence Act¹⁶ in effect, prohibit one from adducing oral evidence to the effect that the terms of a contract, grant or disposition of property.

What then will happen to electronically generated contracts, will the same parole rule apply even if the said oral evidence does not affect the terms and conditions or essence of the contract? This may still pose a challenge in relevance and admissibility of electronic evidence for lack of proband law. Documents under evidence law are considered only admissible in court, provided they are properly authenticated. Several innovations need to be incorporated at parameters for admitting electronic evidence in judicial proceedings within Uganda.

B) The Computer Misuse Act, Cap. 96.

The Act provides for security of electronic transactions and information systems; prevention of unlawful access, abuse or misuse of information systems and for security of electronic transactions.

The Computer Misuse Act does not only provide for offences, preservation of data that has been stored or

processed by means of a computer system,¹⁷ but also suspension of the rules of evidence that tends to render electronic evidence inadmissible for not being in its original form.

The section further provides that such evidence should be allowed as the best evidence that could be obtained in the circumstances.¹⁸ On the other hand the Act seems contradictory basing on the provision under section 29(7), that all other rules of evidence apply without modification. The Act requires that procedures be lawfully exercised in recovering electronic evidence from individuals and organization without breach of the law. Yet such rule of law calls for some levels of uniformity and consistency in the process.

C) The Electronic Transactions Act, Cap. 99

The Electronic Transaction Act provides for the use, security, facilitation and regulation of electronic communications and transactions as forms of communication. It also offers legal certainty in respect of cogency, legal effect and enforceability of information in electronic form.

The electronic transactions Act has connectedness to electronic evidence rather than giving it a general application.

D) Electronic Signatures Act, Cap. 98

The Electronic Signature Act makes provision for the use of electronic signatures in order to ensure that transactions are carried out in a secure environment while establishing a public key infrastructure for authenticity and security of documents and recognizing the different signature creating technologies.

Similar to the Electronic Transactions Act, this Act recognizes electronic signatures as used in electronic transactions and authenticates the same. The challenge remains that the Act is silent on the procedure of having such evidence admitted in court, hence a loophole.

E) The Judicature (Visual-Audio Link) Rules, 2016

¹³ Documentary evidence was defined in the case of *Salau Dean v Republic* [1966] EA 272

¹⁴ *Rodney Mugarura v. Paramount Hospital Kampala Ltd & Dr. Simon Begumisa*, Civil Suit No. of 2021.

¹⁵ Contracts Act Cap. 284

¹⁶ Evidence Act Cap. 8

¹⁷ Section 9 (1) of the Computer Misuse Act, Cap. 96

¹⁸ Section 29 of the Computer Misuse Act, Cap. 96

The Judicature (Visual-Audio Link) Rules are concerned with taking of evidence in court by visual-audio links and making it easier for witnesses to give evidence without physically appearing in court although this does not make the evidence of such a witness electronic as evidence

The use of Visual-Audio Links is merely an administrative channel for expeditious determination of disputes and does not constitute electronic evidence¹⁹ much as it makes it more affordable to use technology to conduct proceedings in courts of law. The rules have only profited bail applications and a few other special circumstances in court hearings.

F) The Constitution (Integration of ICT into the Adjudication Process for Courts of Judicature) (Practice Directions), 2019

The Constitution (Integration of ICT into the Adjudication Process for Courts of Judicature) (Practice Directions), 2019 provide for electronic service of court documents, providing for electronic forms of documents including pleadings, emphasizing use of technology but still no procedure of admitting electronic evidence is mentioned.

G) United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce

Uganda being a dualist State means that international law only forms part of the recognized sources of law²⁰ if only it has been domesticated by legislation or enacted by an Act of the Ugandan Parliament. The UNCITRAL was made in 1996 (and amended in 1998) to assist countries in the framing of legislation and facilitate electronic commerce and electronic government. The model law establishes rules and norms that validate and recognize contracts formed through electronic means, sets rules for forming contracts and governing electronic contract performance, defines the characteristics of valid electronic writing and of an original document, acceptability of electronic signatures for legal and commercial purposes, and

supports the admission of computer evidence in courts and arbitration proceedings.

3. Digital Evidence Challenge, Management, Adaptation and Erasure

As the volume of digital evidence continues to grow exponentially and its importance to the outcome of cases remains critical, a deeper understanding of the nature of these records is required to make meaningful decisions about its authenticity.

Electronic documents can be copied but are also easy to be manipulated, altered, updated and deleted. A case in point; what sup messages, email, instant messaging and internet communications are prone to interference²¹ once computers are networked together, document may be transmitted and different copies distributed and altered by various recipients. Unfortunately, court not being tech-savvy to discern which evidence is authentic has fervently relied on admissibility of certain electronically generated evidence without protest, occasioning miscarriage of justice.

4. Contrary Rulings and Authentication

Courts apply widely different standards for similar types of evidence when computer-generated information and digital images are presented in court. For instance, court may contest a motion for summary judgment owing to the failure to provide admissible evidence and properly authenticate computer-generated evidence²² and assure the accuracy of the records.²³ Applicability of digital data and devices from which electronic evidence is generated raises many difficult evidentiary issues and questions which may be overlooked during court proceeding.

Authentication would mean the genuineness, of the document has to be established. Whether the document is what it purports to be is a matter of

¹⁹ KTA Advocates, supra note 5

²⁰ Article 8(A) of the 1995 constitution of the Republic of Uganda, it provides that Uganda shall be governed on principles of national interest and common good enshrined in the National Objectives and Directive Principles of State Policy (DPSP); of which 'Objective XXVIII (b) of the principles of national objectives and the (DPSP) provides that one of the foreign policy objectives is respect for international law and objectives'.

²¹ 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.

²² Lorraine v. Markel American Insurance Co., 241 F.R.D. 554 (D. Md. 2007).

²³ Vinhnee v. American Express Travel Related Services Company, Inc., 336 B.R. 437 (9th Cir. BAP 2005)

conditional relevance.²⁴ Under electronic record, courts have to establish the author of the records, whether the computer program that generated the records is reliable, altered, manipulated or damaged after they were created and whether the evidence is complete.²⁵

5. Inconsistency with Some Evidential Rules

Inconsistency of electronic evidence with other forms such as the best evidence and hearsay rules creates confusion for the courts. The best evidence rule requires submission of the best form of evidence, usually the original of the documents for instance.²⁶ On the other hand, hearsay precludes the admission of testimony by a person who did not perceive directly that which he or she is attesting to.²⁷ In the M-Pesa case, court ruling stated that printouts automatically generated from the service provider, involving no human intervention could have been taken as real evidence.²⁸ While it may be correct to conclude that digital data has the potential to violate the hearsay rule, it is equally vital to distinguish between the types of digital data one is dealing with.

It's vital to have the officers responsible for seizing information, or a suitable qualified employee from the service provider who attains the information, to be present in court to afford corroboration by way of affidavit or otherwise as to the authenticity of electronically interrelated statements.

6. Storage, Preservation and the High-Cost Challenge

Storage of data in electronic devices, if not properly taken care of viruses may destroy it as a result of mechanical damages that manifest constant updates is a necessity. Even so, when data is regularly getting updated on the data bases and websites there are high chances of losing such evidence or having such evidence change form or originality.

In preservation of evidence, it suffers genuine risk of unreliability due to related hacking or other malicious alterations, yet the courts continue to admit such information into evidence.

Infrastructure involving electronic evidence in over 600 courts in Uganda today²⁹ is costly. Configurations need to be established so that courts are able to disclose electronic evidence. Notably, the cost of investing in such systems are excessive for modest budgets for purposes of e-court technologies as opposed to paper records.

7. Challenges in Admission of Illegally Obtained Evidence

Admissibility is interweaved with legality of the acquisition of the evidence. This necessitates determining if the evidence was collected with the proper permission and authorization tools such as; consent, search warrants, and exigency. Digital investigation just like other entail a warrant to be attained before the evidence can be used to charge the accused person.

Consent is directly related to privacy issues.³⁰ Conversely, with the introduction of privacy legislation, uncertainty has been created in digital forensics about what is acceptable behavior in collecting and retrieving personal information.

8. The Way Forward

Under technological development, evidential practice needs to advance to accommodate electronic evidence. It is arguable that the judiciary themselves might be able to liberate litigants from some of the problems created in the process of tendering of evidence at trials.

In order to make admissibility of electronic evidence effective, it is vital for the courts in Uganda to be computerized so as to allow taking of evidence and writing of rulings and judgments electronically as it has been fully done in other jurisdictions.³¹ Courts should embrace remarkable potentials linked to computer with the aim of improving the Ugandan

²⁴ 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>.

²⁵ Amongin Jane Frances Okili V Lucy Akello CS No.1 of 2014

²⁶ Section 62 of the Evidence Act Cap. 8

²⁷ Sections 58 and 59 of the Evidence Act Cap. 8

²⁸ Mason, S. & Seng, D. (Eds.), Electronic Evidence. (88-100). 4th edn, Institute of Advanced Legal Studies for the

SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

²⁹ <http://judiciary.go.ug/files/downloads/Structure%20and%20Functions%20of%20the%20Judiciary%20-%20CR%202012.pdf>

³⁰ Article 27 of the 1995 Constitution of the Republic of Uganda.

³¹ Countries like Britain, South Africa, and America to mention but a few, have embraced such technology.

judicial system and curb undue delays and denial of justice which is a norm in the Ugandan judicial system.

Ugandan Prosecutors, Judges and Lawyers must obtain and develop necessary skills to be able to deal effectively with the problems that may arise in the admissibility of computer generated evidence. Adoption of sound practices that justify the legal requirements for authenticity, reliability, and integrity are required to cast doubt on the authenticity of electronic evidence.

In electronic evidence, public and private computer experts that could be called upon by the courts to corroborate the evidence before the court when it necessities to do so arises in the course of the court proceeding.

As a mandate the Parliament of the Uganda should from time to time make regulations³² generally proposing further conditions with respect to admissibility of any class of evidence that may be pertinent under the law.

9. Conclusion and Recommendation

While the courts in this digital era continue to struggle with the authenticity of digital evidence, most of them on whatever grounds have found the information admissible. However, this calls for a great degree of technical knowledge of the nature of electronic evidence by all parties through a systematic and scrupulous approach to gathering and presentation of evidence on the part of investigators, auditors, computer managers and lawyers. This will purposely close up the gaps created on validity, reliability and admissibility of evidence by the courts.

References

Books

Mason, S. & Seng, D., *Electronic Evidence*, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 4th ed., 2017, P. 88-100.

Journals

Asanwa. S. Eyiuche et al., *Admissibility of Electronically Generated Evidence in Nigeria: A General overview*, Law and Social Justice Review, Vol.4, No.1, 2023.

IUIU, *Electronic Evidence, A case for Reform of the Law of Evidence in Uganda*, 2019.

J. Ssemuddu, *Electronic Evidence Management: Adoption of Standard Operating Procedure for Admissibility of Electronic Evidence*, 2017.

KIU, *Analyzing the Revelance and Admissibility of Electronicakly Generated Evidence in Ugandan Courts*, 2024.

Uvietobore Emuveyan Enaya, *Admissibility of Electronically Generated Evidence in Nigeria*, No: 090601120.

Legislation

Constitution of the Republic of Uganda 1995

Evidence Act Cap.8

Computer Misuse Act, Cap. 96

Electronic Signature Act Cap. 98

Electronic Transaction Act Cap.99

The Judicature (Visual-Audio Link) Rules, 2016

The Constitution (Integration of ICT into the Adjudication Process for Courts of Judicature) (Practice Directions), 2019

Cases

Amongin Jane Frances Okili V Lucy Akello CS No.1 of 2014

Dian GF International Ltd Vs Damco Logistics Ltd &Trantrack (Civil Suit No. 161 of 2010) [2012]

Lorraine v. Markel American Insurance Co., 241 F.R.D. 554 (D. Md. 2007)

Rodney Mugarura v. Paramount Hospital Kampala Ltd & Dr. Simon Begumisa, Civil Suit No. of 2021.

R v Blackshaw and others [2011] EWCA Crim 2312
Vinhnee v. American Express Travel Related Services Company, Inc., 336 B.R. 437 (9th Cir. BAP 2005)

Report

Vastina Rukimirana Nsaza, *Uganda Law Reform Commission Annual Report on the Law of Evidence*. ALRAESA Conference on 29th – 30th June, 2017.

Online sources

Dian GF International Ltd Vs Damco Logistics Ltd &Trantrack (Civil Suit No. 161 of 2010) [2012] Accessible on

³² Article 79 of the 1995 Constitution of the Republic of Uganda.

<https://ulii.org/ug/judgment/commercial-court/2012/10>. Accessed on 10 March, 2025.

Electronic Evidence, George, Madison University of London Press, Institute of Advanced Legal Studies, 2017. Accessible via <https://www.jstor.org/stable/j.ctv512x65>. Accessed on 10 March, 2025.

<http://judiciary.go.ug/files/downloads/Structure%20and%20Functions%20of%20the%20Judiciary%20-%20CR%202012.pdf>. Accessed on 10 March, 2025.

<https://ulii.org/ug/judgment/commercial-court/2012/10>. Accessed on 21 March, 2025.

KTA Advocates, Electronic Evidence, Legal Alert, 2019. <https://www.ktaadvocates.com/wp-content/uploads/2020/10/ELECTRONIC-EVIDENCE-LEGAL-ALERT-KTA.pdf>. Accessed on 28 June, 2026.