ARTICLE:

The admissibility and authentication of digital evidence in Zanzibar under the new Evidence Act

By **Alex B. Makulilo**

The rise and development of digital technology has profound effect on legal concepts and rules in many legal systems. In the field of evidence, the widespread use of modern technologies in our daily lives has created and generated materials that are considered evidence in courts. As a result, the outcome of civil and criminal trials increasingly hinges around the production of digital evidence in legal proceedings. This article casts light on the standards of admission and authentication of electronic evidence in courts under the new Zanzibar Evidence Act 2016, which came into force on 18 January 2017. As pointed out by Schafer and Mason, electronic evidence can include both analogue and digital evidence. Both terms are used interchangeably in this article.[1]

Introduction

Zanzibar is part of the United Republic of Tanzania. The latter is made up of the former Republic of Tanganyika (now Mainland Tanzania) and Republic of Zanzibar. However Zanzibar has its own executive (the Revolutionary Government of Zanzibar) and parliament called the Zanzibar House of Representatives, which deal with non-union matters for Zanzibar.[2] The judiciary in Zanzibar is also a non-union matter except at the level of the Court of Appeal of Tanzania. This means that appeals from the High Court of Zanzibar are heard and determined in the Court of Appeal of Tanzania.[3] Historically, both Zanzibar and Tanganyika were once under the British colonial rule, inheriting the common law legal system, which prevails to date.

Under the common law legal system, the admissibility of evidence depends on the rules of authentication, hearsay and the best evidence rule. These rules were codified in the now repealed Evidence Decree (Cap. 5 of the Laws of Zanzibar) at the time of analogue technology. The rise of digital technologies and their application has challenged the application of the common law rules of evidence. This challenge is demonstrated in the landmark case of *Salum Said Salum v DPP*,[4] where the High Court of Zanzibar had to consider the admissibility of Video Compact Disc (VCD) and whether such technologies came within the definition of document in section 3(1) of the Evidence Decree. The latter states that 'document' means:

> '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, for the purpose of recording that matter.'

Since this definition made no reference to evidence in digital form, the court had to reference foreign law to assist it to decide this question. To ensure authenticity of the VCD prior to its admission, the court developed three guidelines: the VCD must be accurate; the voices and picture must be properly identified, and the VCD must be relevant to the issues in the litigation.

[1] Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence', in Stephen Mason and Daniel Seng editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), 2.3 – 2.9.

[2] Non-union matters refer to all the matters that are not listed in the First Schedule of the Tanzanian Constitution, Cap.2 R.E 2002.

[3] According to Article 114 of the Tanzanian Constitution, the Judiciary in Zanzibar comprises the High Court and subordinate courts, which include Kadhis Court. The subordinate courts include at the lowest level, the Primary Magistrate court, District Magistrate court and Regional court. The Industrial Court has jurisdiction to hear and to determine labour disputes. The Industrial Court is the division of the High Court of Zanzibar.

[4] High Court of Zanzibar, Criminal Appeal No. 3 of 2013, HCZ, Vuga (unreported), available at http://www.judiciaryzanzibar.go.tz/judgement/high_court/Criminal%20App%20No%2003%20of%202013%20Salum%20Said%20Salum%20vs%20DPP%20-%20Electonic%20Evidence.pdf .

The point that clearly emerges from this case is that by its nature, digital evidence differs significantly from conventional evidence.[5] These differences limit the application of the common law rules of evidence. For example, in contrast to non-digital forms of evidence, digital evidence is never in a form readable by humans. Evidence in digital form depends primarily on machinery and software to be rendered into human-readable form.[6] Digital data is represented in the binary form, that is, 0s and 1s. No one would understand this machine language. Accordingly additional steps are required to include digital documents as evidence (e.g. displaying on a computer screen or printing out the material). This change of form has challenged the application of the best evidence rule,[7] which requires the content of a document to be proved by tendering an original. Central to the difficulties of application of the best evidence rule are issues surrounding identification of the primary evidence of a digital document.[8] There have been conflicting views on this point: the first school of thought holds that the memory or database of a word-processor or computer is the original document (including software and binary code) presumably because these are components on which material fed into a simple word processor is stored.[9] In contrast, the second school of thought led by Tapper holds the view that the print-out from the word-processed electronic document is the original and the document in the memory computer is the copy.[10] Mason and Seng argue that both views are possible, although the approach in the first school of thought is plausible. This is due to the fact that the print-out is generated as a physical draft to aid in the editing of the word-processed document.[11]

The other problem relates to the authentication of digital evidence. The latter means it might be necessary to satisfy the court that the contents of the record have remained unchanged, that the information in the record does in fact originate from its purported source, whether human or machine, and that extraneous information such as the apparent date of the record is accurate. The challenge to the authentication of digital evidence is that digital data is easy to replicate, copy, alter and disseminate and it is possible to make additions or deletions that are not apparent to viewers of the documents. Accordingly, it may be difficult to establish the precise document that the parties rely upon. This necessarily implies a higher threshold level of authentication of digital evidence is required. Conversely, most electronic evidence has been accepted in courts without any suspicion – the real problem here is the ignorance of the judges and lawyers who fail to appreciate the unique characteristics of digital evidence and insist on applying both the common law rules and legislative provisions embodying guidelines that were developed around paper documents.[12] It is worthy to note the five tests for authentication of digital evidence are now included in the Draft Convention on Electronic Evidence which was published in 2016, for which see below.[13]

Hearsay is also problematic. Mason has demonstrated legal issues surrounding the hearsay rule in 'Software code as the witness'.[14] The core question is whether digital evidence should be treated as a joint statement partly made by the person inputting data (such as typing an e-mail or word document, inserting a PIN, filling in forms over the internet – in essence anything a person does when interacting with a devices), and partly made by the hundreds of programmers who are responsible for writing the software that produces the data. Mason classifies digital data as either content written by one or more people (e.g. e-mail messages, word processing files and instant messages), records generated by software that have not had any input from a human (e.g. computer data log and records of ATM transactions), or records comprising a mix of human input and calculations generated by software (e.g. financial spreadsheet programme that contain human statements and computer processing). In any case, the question might be which part of the joint statement is hearsay and which one is real evidence.

[5] For a comprehensive discussion, see Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence', in *Electronic Evidence*, ch 2.
[6] *Electronic Evidence*, 21 – 22.
[7] The best evidence rule is a rule of evidence that requires an original document, photograph, or other piece of evidence be introduced to the court to prove the contents of that same item.
[8] Stephen Mason and Daniel Seng, 'The foundations of evidence in electronic form' in *Electronic Evidence*, ch 3, 53 – 55.
[9] See e.g., *Derby v Weldon* (No.9)[1991] 2 All ER 901, 906.
[10] Stephen Mason and Daniel Seng, 'The foundations of evidence in electronic form', *Electronic Evidence*, ch 3, 53.
[11] Stephen Mason and Daniel Seng, 'The foundations of evidence in electronic form', *Electronic Evidence*, ch 3, 53.
[12] For a comprehensive discussion read Stephen Mason and Allison Stanfield, 'Authenticating electronic evidence' in *Electronic Evidence*, ch 7.
[13] 13 *Digital Evidence and Electronic Signature Law Review* (2016), S1 – S 11, available at http://journals.sas.ac.uk/deeslr/article/view/2321 .
[14] Stephen Mason, 'Software code as the witness' in *Electronic Evidence*, ch 5.

This has generated a debate among legal scholars. Perhaps to address the problem of hearsay, legislation and case law puts a number of exceptions to the general rule against hearsay. The most important one is the business record exception discussed below. However, there remain problems when the business record exception is applied in the context of digital records.[15]

International law on the admission and authentication of electronic evidence

UNICITRAL Model Laws

There is no international treaty on the subject of electronic evidence. However, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (Guide to enactment with additional article 5 bis as adopted in 1998), provides legislative guidance at the United Nations level for countries to develop their national law.

The rules in the Model Law have been influential in legal reforms of evidence legislation in many jurisdictions. The Model Law is guided by the functional equivalent approach. The latter is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. Accordingly, article 5 makes a general recognition of a data message as follows:

> 'Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.'

Article 2(a) of the Model Law provides the meaning of a 'data message' as follows:

> 'a data message means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.'

The Model Law also provides for the requirements of writing in article 6(1), which states that

> 'Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.'

As regards to the original, the Model Law provides, under article 8(1):

> '(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
>
> (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
>
> (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.'

The signature is an important method of authentication of evidence, and the Model Law provides, in article 7(1):

> '(1) where the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.'

The fundamental principle of evidence in the Model Law is that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, as provided for in article 9(1).

The Model Law provides further that information in the form of a data message shall be given due evidential weight, as provided in article 9(2):

> 'In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was

[15] Note the vignette 'Business records' in *Electronic Evidence*, xii – xiii.

> generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.'

The other important international framework is the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures with Guide to Enactment 2001. It provides guidance to countries on how to develop their national laws on this subject. Essentially, the UNCITRAL Model Law on Electronic Signatures provides for authenticity of a person using electronic signature, although it also provides for the integrity of a message or document. The UNCITRAL Model Law on Electronic Signatures is a detailed framework that expands article 7 of the UNICITRAL Model Law on Electronic Commerce.

Draft Convention on Electronic Evidence

A private initiative recently produced a Draft Convention on Electronic Evidence.[16] This draft Convention deals with, among other issues, the authentication of electronic evidence and the application of the best evidence rule. The draft Convention is very useful and is a good starting point of understanding the rules of evidence as applicable in digital form.

The draft Convention defines the term computer as any device capable of performing mathematical or logical instructions. This definition is broad, and may include smartphones, ATM machines, digital watches, etc. It also defines electronic evidence in article 1 as:

> 'evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network.'

Another important definition in the draft Convention is an electronic record, which is also defined in article 1 as:

> 'data that is recorded or stored on any medium in or by a device programmed by software code and that can be read or perceived by a person or any such device, and includes a display, printout or other output that represents the data.'

With regard to the rules of admissibility of electronic evidence, article 2(2) of the draft Convention states that it does not modify any existing national rule that applies to the admissibility of evidence, except in relation to the rules relating to authenticity and best evidence. The latter are covered in part one of this article. It is important to mention that the draft Convention is a useful guide for the authentication of digital evidence and could be adopted in Zanzibar without any political or legal problems. This is due to a number of reasons. First, legal transplants have a long history in Tanzania generally and in Zanzibar in particular. During the past century, legal transplants took place mainly because of colonization.[17] The British colonial power occupied Zanzibar and Tanganyika, importing its common law legal systems and norms. After independence, legal transplants are the main cause of trade-related legal changes in the developing world.[18] Many developing countries have been pushed to create a more stable environment that conforms to the standards existing in developed markets. Second, as part of the international organisations such as the United Nations and World Trade Organisation, Zanzibar is obliged to develop certain legal standards through what is called voluntary legal transplantations that aim to harmonize the legal norms worldwide in order to enhance trade and reduce dispute among nations. It is argued that legal convergence has been taking place worldwide due to development of modern technologies that have facilitated international business through electronic commerce and increased interactions among people. Indeed the High Court of Tanzania has held in *Trust Bank Tanzania Ltd v Le-Marsh Enterprises Ltd and Others*[19] that:

> 'Tanzania is not an island by itself. The country must move fast to integrate itself with the global banking community in terms of

[16] 13 *Digital Evidence and Electronic Signature Law Review* (2016), S1 – S 11, available at http://journals.sas.ac.uk/deeslr/article/view/2321 ; Stephen Mason 'Towards a global law of digital evidence? An exploratory essay', *Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 103, Autumn 2015, 19 – 28, available at http://journals.sas.ac.uk/amicus/article/viewFile/2481/2439 .

[17] Federico Baldelli, Legal Origins, *Legal Institutions and Poverty in Sub-Saharan Africa*, LUISS Guido Carli University, Master of Science in Law and Economics, 2010, p. 38.

[18] Federico Baldelli, *Legal Origins, Legal Institutions and Poverty in Sub-Saharan Africa*, LUISS Guido Carli University, Master of Science in Law and Economics, 2010, p. 39.

[19] *Trust Bank Tanzania Ltd v Le-Marsh Enterprises Ltd and Others* [2002] T.L.R 144.

> technological changes and the manner in which banking business is being conducted. The courts have to take due cognisance of the technological revolution that has engulfed the world. Generally speaking as of now, record keeping in our banks is to a large extent "old fashioned" but changes are taking place. The law can ill afford to shut its eyes to what is happening around the world in the banking fraternity. It is in this spirit that I am prepared to extend the definition of banker's books to include evidence emanating from computers.'[20]

In the *Trust Bank* the High Court of Tanzania referenced its decision on the UK Bankers Books Evidence Act 1879 as amended in 1979 as well as case law such as *Barker v Wilson.*[21] The High Court of Zanzibar has similarly followed the approach by the High Court of Tanzania where it had to reference its decision in *Salum Said Salum v DPP* to the UK law. This demonstrates lack of resistance in legal transplantation. Third, the Zanzibar new Evidence Act requires the Chief Justice to develop rules on authenticity of evidence and digital signature among other things. Since the draft Convention provides for these rules, which are drafted to be totally neutral, Zanzibar may seek guidance from it.

Southern African Development Community Model Law on Electronic Transactions and Electronic Commerce

In Africa, the Southern African Development Community (SADC) has a framework of the law on electronic evidence. This is called the SADC Model Law on Electronic Transactions and Electronic Commerce 2012, which is also applicable to Zanzibar as it is a member of SADC through the United Republic of Tanzania. The SADC Model Law has the same provisions as the UNCITRAL Model Law on Electronic Commerce [Article 20(1)-(3)]. In addition, the SADC Model Law on Electronic Transactions and Electronic Commerce incorporates a business record exception in article 20(4). This provision states:

> 'An electronic communication made by or on behalf of a person in the ordinary course of business, or a copy or printout of, or an extract from such electronic communication certified to be correct, is admissible in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, as evidence of the facts contained in such record, copy, printout or extract against any person, provided:
>
> a. the affidavit is made by the person who was in control of the system at the time when the electronic communication was created;
>
> b. the affidavit contains sufficient information on the following:
>
> i. the reliability of the manner in which the electronic communication was generated, stored or communicated;
>
> ii. the reliability of the manner in which the integrity of the electronic communication was maintained;
>
> iii. the manner in which the originator of the electronic communication was identified; and
>
> iv. the reliability of the information system.'

It is interesting to note that neither the African Union Convention on Cyber Security and Personal Data Protection 2014 (EX.CL/846(XXV), nor the Economic Community of West African States (ECOWAS) framework on e-transactions 2010 ((Supplementary Act A/SA.2/01/10) contains rules or guidelines as to admissibility of electronic evidence. This means that the influence of the African Union and regional economic groups is minimal when it comes to the national development of electronic evidence legislation.

[20] *Trust Bank Tanzania Ltd v Le-Marsh Enterprises Ltd and Others*, 148-149.
[21] *Barker v Wilson*[1980] 2 All ER 80.

Legislative history of the Zanzibar Evidence Act

The Zanzibar Evidence Decree was the principle legislation that governed the rules of evidence in courts in Zanzibar, adopted in 1917 long before the independence of Zanzibar. It remained unchanged for several decades. The first challenge that brought the limitation of the Evidence Decree to the attention of the courts in the context of digital evidence is the case of *Salum Said Salum v DPP*. The main legal question in that case was whether digital evidence was admissible in Zanzibar under the Evidence Decree. The High Court of Zanzibar answered this question positively. However, the judges looked to Indian case law in considering this question, where the English common law legal system was first adopted.

After *Salum Said Salum v DPP*, and similar case law in mainland Tanzania as well as legislative attempts to address the challenges of digital evidence, the Parliament of the United Republic of Tanzania passed the Electronic Transactions Act 2015.[22] This Act incorporates, in Part IV, a regime of rules that governs the admissibility of digital evidence in courts. It is important to point out at the outset that the Electronic Transactions Act is union law. It applies both to mainland Tanzania and Zanzibar. However, according to the provisions of article 150 of the Constitution of the United Republic of Tanzania (as amended from time to time), a union law does not directly apply to Zanzibar until it is laid before the House of Representatives. The Electronic Transactions Act has never been laid before the Zanzibar House of Representatives. Accordingly it is not applicable on Zanzibar at the moment.

Instead, in 2016 Zanzibar repealed its Evidence Decree and replaced it with the new Zanzibar Evidence Act No 9 of 2016.[23] This Act incorporates a special body of rules in sections 72 and 73, which exclusively apply on digital evidence. It is noteworthy that sections 72 and 73 of the Evidence Act are totally identical to sections 65A and 65B of the Indian Evidence Act as amended by the Information and Communication Technology Act 2000. It is also important to note that the Indian law is based upon the United Kingdom Civil Evidence Act 1968. The latter was repealed in 1995 just before the Indian Evidence Act was amended. Similarly, the Zanzibar Evidence Act is partly based on section 40A of the Written Laws (Miscellaneous Amendments) Act 2007 which amended the Mainland Tanzanian Evidence Act Cap.5 R.E 2002 as far as electronic evidence in criminal proceedings is concerned. This section is identical to section 42 of the Zanzibar Evidence Act.

Anatomy of the Evidence Act with regard to digital evidence

New definitions

The Evidence Act introduces new definitions of legal concepts to accommodate digital evidence. First, the Act defines, in section 3, the term computer as:

> 'an electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network'

The above definition is not confined to the traditional desktop computer. It includes any data processing device that uses software to perform its functions. For the purposes of this definition, a smartphone, an automated teller machine (ATM), and a blood pressure machine are all examples of a computer under the new Zanzibar Evidence Act.

The Evidence Act re-defines the term document under section 3:

> 'means any writing, handwriting, typewriting, printing, Photostat, photograph and every recording upon any tangible thing, any form of communication including electronic document, communication or representation by letters, figures, marks or symbols or by more than one of these means, which may be used for the purpose of recording any matter provided that such recording is reasonably permanent and readable by sight'

[22] For a comprehensive evolvement of electronic evidence law in Tanzania and its application, see Alex B. Makulilo, 'The admissibility of electronic evidence in Tanzania: new rules and case law', 13 *Digital Evidence and Electronic Signature Law Review* (2016), 109 – 120; The Electronic Transactions Act, 2015, available at http://mwtc.go.tz/uploads/publications/en1473250962-sheria-the_electronic_transactions_act_-_final.doc.pdf .

[23] The Zanzibar Evidence Act, 2016, available at http://www.zanzibarassembly.go.tz/act_2016/act_9.pdf .

A definition of electronic document is provided in section 3 of the Act:

> 'electronic document means a message, instrument, information, data, text, program, software, database, or the similar item, regardless of how created, if such item can be retrieved or displayed in a tangible form'

According to this definition, electronic evidence includes documentary evidence under the Evidence Act. This might further suggest that the common law rules of documentary evidence generally stated in the Evidence Act are applicable when there are issues of admissibility of electronic evidence in court. However, this is not the case, because the Act clearly provides special provisions in sections 72 and 73 of the Evidence Act govern the admissibility of all electronic evidence. There is therefore little room for the application of the common law rules of evidence in the admissibility of electronic evidence.

The Act defines electronic records in section 3 as:

> 'any record which is created, generated, sent, communicated, received, or stored by electronic means;'

Illustrations of electronic records may include: e-mail messages, text massages, word- processed documents, electronic spreadsheets, digital images and databases.

The Evidence Act also defines documentary evidence in section 3 as:

> 'all documents including electronic records produced for the inspection of the Court;'

This means that every electronic document constitutes a record and every record constitutes document and is therefore documentary evidence.

Application to legal proceedings

In accordance with the provisions of section 2, the Evidence Act applies to all judicial proceedings in or before any court. Furthermore, section 42 of the Act specifically refers to evidence of surveillance in criminal proceedings. This provision states as follows:

> 'In any criminal proceedings:
>
> (a) an information retrieved from computer systems, networks or servers shall be admissible in evidence;
>
> (b) the records obtained through surveillance of means of preservation of information including facsimile machines shall be admissible in evidence, electronic transmission and communication facilities; or
>
> (c) the audio or video recording of acts or behaviours or conversation of persons charged
>
> shall be admissible in evidence.'

It is interesting to note that section 42 of the Evidence Act attempts to create a special regime of admissibility of digital evidence in criminal proceedings. However, this might not be the case, since sections 72 and 73 of this Act (discussed below) lay down special provisions as to the admissibility of electronic records irrespective of the type of proceedings. In the author's view, section 42 is redundant, because electronic evidence may only be admitted in the Evidence Act subject to the provisions of sections 72 and 73. In any case, section 42 does not provide for the conditions and criteria for admissibility of electronic evidence.

Business record exception – the default rule for admissibility of electronic evidence

The marginal notes to section 72 of the Evidence Act provide that this section is about special provisions relating to electronic records. Section 72 states that the contents of electronic records may be proved in accordance with the provisions of section 73. Sections 73(1) and (2) of the Evidence Act provide as follows:

> '(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer hereinafter referred to as the computer output, shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question 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.

(2) The conditions referred to in subsection (1) of this section in respect of a computer output shall be the following:

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during that period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of those activities;

(c) throughout the material part of that period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of those activities.

Proof only by certificate

The Evidence Act requires in section 73(4) that every piece of electronic evidence must be proved by way of certificate. The relevant provision states:

'(4) In any proceedings where it is desired to give statement in evidence by virtue of this section, a certificate doing any of the following:

(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; or

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) of this section 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 the matter stated in the certificate; and for the purposes of this section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.'

It is important to underline that the certificate envisaged under section 73(4) of the Act must be signed by a person occupying responsible official position in an organisation (e.g. IT administrator) or a person in the management position. This is typically a requirement in the authentication of digital evidence with respect to business records.

Requirement for a digital signature

Section 76 provides that a digital signature must be proved with reference to its subscriber, except in the case of a secure digital signature. Under section 83 the court may direct that the digital signature provider or authority produce the Digital Signature Certificate for purposes of such proof. It may also direct any other person to apply the public key listed in the Digital Signature Certificate and verify the signature purported to be affixed by that person. It is important to note that authentication by way of digital signature is to be regulated by rules made by the Chief Justice under section 184(2)(a) of the Evidence Act.

Presumptions

The Act provides for a number of presumptions:

(i) A secure electronic record is presumed to not have been altered since the specific point of time to which the secure status relates, unless the contrary is proved (s98 (1)).

(ii) The court may presume that a secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record [s98 (2)].

(iii) The information listed in a Digital Signature Certificate is presumed as

correct (s99).

(v) The court may presume as proved communication of electronic message originating from a telecommunication office (s102).

(vi) The court may presume as proved an electronic message forwarded by the originator through electronic mail server to the addressee (s103).

(vii) The court may presume as proved a digital signature that is five years old and produced from custody (s106).

Rules of the Chief Justice

Section 184(1) provides that the Chief Justice may make rules to carry out the provisions of this Act. This power is general and may relate to any provision of the Act. Subsection 2 provides a non-exhaustive list of such rules:

> '(a) the manner in which any information or matter may be authenticated by means of digital signature;
>
> (b) the manner and format in which electronic records shall be filed, tendered or issued before the court;
>
> (c) the matters relating to the type of digital signature, manner and format in which it may be affixed;
>
> (d) the security procedure for the purpose of creating secure electronic record and secure digital signature;
>
> (e) any other matter which is required to be, or may be, prescribed.'

However, the Chief Justice has yet to make any Rules.

Analysis of the special provisions of digital evidence

The main problem with the new Evidence Act lies in its drafting, especially with respect to the special provisions regarding electronic evidence. As previously pointed out, sections 72 and 73 of the Zanzibar Evidence Act 2016 are identical to sections 65A and 65B of the Indian Information Technology Act 2000. It is interesting to note that the two sections of the Indian Information Technology Act 2000 reflect section 5(2) of the UK Civil Evidence Act 1968, which was repealed in 1995. The reason why section 5 of the Civil Evidence Act 1968 was repealed is that it was enacted at the time mainframe computers were in regular use by organisations. Accordingly, section 5 of the Civil Evidence Act 1968 was meant to regulate admission of electronic records emanating from mainframe computers that were largely used by organisations. Due to this, it is argued that sections 72 and 73 of the Zanzibar Evidence Act are capable of operating to exclude wide categories of electronic documents. This is because, for an electronic record to be admitted under sections 72 and 73 of the Act, it must fall within the class of business record which is a result of a regularly conducted activity by an organisation [section 73(2)(d)] such as a bank. Electronic records of day-to-day communications and other documents that cannot be categorised, as business records may not be admitted under these provisions. This argument is strengthened by the requirement of proof by certificate in section 73(4) that 'purports 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' in proving any of the conditions in section 73(2) of the Evidence Act. With these requirements, it is not clear how an alleged defamatory WhatsApp message sent to a WhatsApp group by a group member will meet such conditions: business records and proof by certificate.

Professor Reed makes similar remarks on section 5(2) of the Civil Evidence Act 1968, which is identical to sections 65B and 73(2) of the Indian Information Technology Act 2000 and the Zanzibar Evidence Act 2016 respectively:

> 'These four conditions show the age of the legislation. They are aimed primarily at the batch processing of identical transactions, and the type of computer operation envisaged by the legislature is clearly a substantial mainframe operation which is processing hundreds or thousands of similar transactions daily. However, the widespread introduction of microcomputers in recent years means that the types of information stored are far more diverse, and the regularity with which

> information of that type is recorded is less frequent, than would have been the case with mainframe systems of the mid-1960s. There is thus some doubt whether free-form databases or information contained in word-processed documents will, at least in precise terms, comply with these four conditions.'[24]

Related to the problem of exclusion of certain categories of digital evidence (i.e. non-business records) from the scope of sections 72 and 73 of the Evidence Act, are several misconceptions on the part of the drafters of concepts and principles which apply to digital evidence.

Sections 72 and 73 of the Zanzibar Evidence Act govern proof of electronic records. Section 72 does nothing more than point out that proof of electronic records shall be done in accordance with the provisions of section 73 of the Evidence Act. Overall, these provisions take precedence over other provisions in the Act as far as admissibility of electronic evidence is concerned. To be sure, section 73(1) of the Evidence Act begins with the following words 'notwithstanding anything contained in this Act', meaning that compliance with the special provisions for the admissibility of electronic records is therefore a prerequisite for all computer-produced documents.

A critical review of section 73(1) of the Act reveals that it aims at addressing two issues. First, it deems every computer output either in the form of a printout or display or any other form to be a document. Of course, this might be a repetition of the definitions of document, electronic document and electronic record in section 3 of the Evidence Act. Secondly, this provision states that any computer output is deemed to be an original document, in which case it shall be admissible without further proof or production of the original. This provision has missed an important point – that there can be no original of an electronic document.[25] The better view could simply be that the computer output will be admissible in evidence as a copy. It is arguable that when the notion of 'original' is introduced the way it is in section 73(1), it fails to appreciate the nature of digital data and hence electronic evidence.

On the other hand, section 73(2) of the Evidence Act provides for the pre-conditions for the admissibility of documents produced by computers. The four conditions in section 73(2) are set out above. A critical review of sections 73(1) and 73(2) of the Evidence Act suggests such conditions are meant in the first place to qualify computer output as document. This section is framed in such a way that a computer output is deemed to be a document the moment it fulfils the conditions under section 73(2) of the Evidence Act 2016. This assumption is wrong. It is submitted that the drafters of the legislation have failed to understand that conceptually, they should have got rid of the similarity to paper documents.

There is yet another serious problem with the drafters of the Evidence Act, especially with regard to the condition set out in section 73(1)(c). The underlying phrase in this sub-section is 'operating properly' with reference to a computer. There are significant problems with regard to this sub-section. First, there is lack of definition in the Act of what is meant by 'operating properly'. The difficulty of interpretation is likely to arise because a computer might be operating 'properly' but not in the way an owner expects, and a third party can instruct a computer to do things that the owner neither authorizes nor is aware of.[26]

The second problem relates to the nature of the presumption created in section 73(2)(c) of the Evidence Act. According to this sub-section, there is a presumption if there is no fault in the computer software at the material time a digital record is created, the output of the computer is regarded as accurate as long as it was produced in the ordinary course of the business of the organisation. Concomitantly, the assertion of reliance becomes sufficient to establish the authenticity of such digital data. This is completely wrong because digital data has always never been trusted due to software errors of the systems they create them.[27] It is therefore necessary when considering evidence tendered under the business records exception (as it is now the case with section 73 of the Zanzibar Evidence Act 2016), to be aware that errors can and do occur-accidentally, deliberately, or because of the failure of the

[24] Chris Reed, 'The Admissibility and Authentication of Computer Evidence – A Confusion of Issues', *Computer Law and Security Report*, Vol. 2, 1990-91, 13 – 16.

[25] For detailed discussion, see Stephen Mason, 'Electronic evidence and the meaning of 'original'', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, Issue 79, Autumn, 2009, 26 – 28, http://sas-space.sas.ac.uk/2565/1/Amicus79_Mason.pdf .

[26] See Stephen Mason, 'The presumption that computers are 'reliable'', *Electronic Evidence*, ch 6, 182.

[27] 'Authenticating electronic evidence', *Electronic Evidence*, ch 7, 254.

software.[28] A fundamental problem is caused by the fact the software errors can be present (in large numbers), but not observable in use until a specific situation is encountered.[29] Accordingly, it will not always be obvious whether the reliability of the evidence generated by a computer is immediately detectable without recourse to establishing whether the software code is not at fault.[30] This calls for evidence surrounding the computer system as such in which the records were created and stored.[31] Although section 73(4) of the Zanzibar Evidence Act attempts to require evidence from an IT administrator *or* a member of staff in the management of the relevant activities of an organisation when proving any of the conditions in section 73(2), it is arguable that both IT administrator and staff in the management of relevant activities of the organisation may need to be obtained. The IT administrator will normally lead evidence as to the security and integrity of the computer system which generated and stored the digital data, while the employee in the management of the relevant activities of the organisation will give evidence as to the content of the digital data generated and stored in the system.

The third problem of the presumption in section 73(2)(c) of the Evidence Act is that it asserts something positive. The opposing party is required to prove a negative in the absence of relevant evidence from the program or programs that are relied upon.[32] This evidential burden, which is placed on the opposing party, becomes difficult to discharge, as the only party in possession of electronic evidence has the ability to understand fully whether the computer or computers from which the evidence was extracted can be trusted.[33]

It is submitted that due to the fundamental problems pointed out, the presumption in section 73(2)(c) of the Evidence Act should be re-considered and in particular be removed. Instead, evidence as to the reliability of the computer (or software) is required as is the case with article 20(4)(b)(iv) of the SADC Model Law on Electronic Transactions and Electronic Commerce 2012. Of course, not every case will need proof of reliability of the computer. This will probably apply in the complex networked systems such as banking systems and the like. In its current form, it might also be right to have the presumption as an aid in the authentication of the evidence-provided the basic facts are proved.[34]

Admissibility of electronic evidence in criminal proceedings

Section 42 of the Zanzibar Evidence Act is identical to section 40A of the Tanzania Evidence Act as introduced by the Written Laws (Miscellaneous Amendments) Act 2007. Both of them deal with admissibility of evidence obtained through undercover operations. The High Court of Tanzania has, over and again, affirmed that section 40A is only applicable to admissibility of electronic evidence in criminal proceedings.[35] However, following the enactment of the Electronic Transactions Act 2015, the High Court of Tanzania has held that the admissibility of electronic evidence in all proceedings must comply with sections 18(1) and 18(2) of the Act.[36] Although the court did not expressly say so, section 40A of the Written Laws (Miscellaneous Amendments) Act 2007 has become redundant. This may also be the case for Zanzibar based on the requirement of the new law. It is now settled that electronic records are admitted under sections 72 and 73 of the Zanzibar Evidence Act. These provisions do not make any distinction between civil and criminal proceedings. It is argued that the drafters of the Zanzibar Evidence Act borrowed section 40A of the Written Laws (Miscellaneous Amendments) Act 2007 without full understanding of the legal implication and scope of sections 72 and 73 of the Evidence Act, thereby making section 42 of the Act redundant.

[28] 'Authenticating electronic evidence', *Electronic Evidence*, ch 7, 254.
[29] Stephen Castell, 'Computers trusted, and found wanting', *The Computer Law & Security Report*, 1993, Vol.9, p. 155.
[30] 'The presumption that computers are 'reliable'', *Electronic Evidence*, ch 6, 182.
[31] 'Authenticating electronic evidence', *Electronic Evidence*, ch 7, 252.
[32] 'The presumption that computers are 'reliable'', *Electronic Evidence*, ch 6, 183.
[33] 'The presumption that computers are 'reliable'', *Electronic Evidence*, ch 6, 180.
[34] 'The presumption that computers are 'reliable'', *Electronic Evidence*, ch 6, 179.
[35] See, e.g., *Lazarus Mirisho Mafie and M/S Shidolya Tours & safaris v Odilo Gasper Kilenga alias Moiso Gasper*, Commercial Case No.10 of 2008, HCT (Commercial Division), Arusha (Unreported), p.24; *Exim Bank (T) Ltd v Kilimanjaro Coffee Company Limited*, Commercial Case No.29 of 2011, HCT (Commercial Division), Dar es Salaam (Unreported), p.5; *Emmanuel Godfrey Masonga v Edward Franz Mwalongo*, Miscellaneous Civil Cause No.6 of 2015, HCT (Iringa District Registry), Njombe (Unreported), p.12.
[36] See, *Emmanuel Godfrey Masonga v Edward Franz Mwalongo*, Miscellaneous Civil Cause No.6 of 2015, HCT (Iringa District Registry), Njombe (Unreported); *William Joseph Mungai v Cosato David Chumi*, Miscellaneous Civil Cause No. 8 of 2015, HCT (Iringa District Registry), Iringa (Unreported).

Authentication of electronic evidence

The other important point relates to authentication of electronic evidence. The Evidence Act provides some guidance with regard to the authentication of electronic evidence. However, the conditions set out in section 73 of the Evidence Act may not adequately cover a wide range of electronic evidence. This is because the conditions for authentication provided in the Act are based upon the fact that the law deals with evidence of business records. Authentication of evidence beyond business records is not specifically provided for. In the latter case, the court will certainly continue to be guided by *Salum Said Salum v DPP* in appropriate cases. Moreover, the court may still be persuasively guided by decisions of higher courts in foreign jurisdictions.

Lack of digital signature rules in the Act

A digital signature is one of the methods by which authentication of electronic document may be achieved in an electronic environment. A digital signature is required to be authentic, secure, not capable of being forged, verifiable, incapable of being re-used and incapable of being altered without rendering the signature unverifiable.[37] These attributes of a digital signature make it stronger than a manuscript signature, although both of them serve the same purpose in the domains of their applications. From a technological point of view, a digital signature uses the application of cryptography that essentially employs a pair of public and private keys to encrypt and decrypt digital information.[38]

It is interesting to note that authentication of evidence by electronic and digital signatures is yet to be regulated in Zanzibar. Section 184(2) (a) of the Zanzibar Evidence Act provides that the Chief Justice shall make rules regarding the manner in which any information or matter may be authenticated by means of a digital signature. The Chief Justice has yet to make these rules. It is argued that provisions as to digital signatures ought to have been incorporated in the Act. This would have solved the problem of waiting for another authority to set out the rules. As the situation stands now, it is difficult to authenticate digital information in the absence of the law. Similarly, in terms of value, having digital signatures stipulated in the Act would make them more stable than in the regulations which are made by authorities other than the legislature hence can be easily changed any time. In this case an amendment of the Evidence Act is proposed to incorporate digital signature. Furthermore, it is recommended that the UNCITRAL Model Law on Electronic Signatures be adopted as guide for the legislative reform in this aspect.

Conclusion

The current technological developments have changed our ways of business practices and communications. Concomitantly, such developments have challenged the existing basic legal concepts and rules of evidence. Different jurisdictions have adopted new legislation or special provisions in their evidence legislation in order to accommodate electronic records in their legal systems. Zanzibar is not an exception. The new Zanzibar Evidence Act 2016 creates a special regime of rules for admission of electronic evidence. The rules provide minimum certainty in the admission of electronic records. Moreover, the exercise of powers to make rules by the Chief Justice under the Act is likely to streamline the operation of the Evidence Act. However, since such rules are subsidiary legislation, they may not provide conditions beyond the parent Act. In this case, it is highly recommended that the legislative shortcomings pointed above should be addressed by way of amendment of the Zanzibar Evidence Act. The Draft Convention on Electronic Evidence that governs admissibility and authentication of electronic evidence may provide a useful starting point.

Alex B. Makulilo, Professor of IT Law, the Open University of Tanzania, LL.B (Dar); LL.M in ICT Law (Oslo); Dr.jur. (Bremen); Postdoc (Bremen). Makulilo is also an Advocate of the High Court of Tanzania and Chairperson of the African Law and Technology Institute.

alex.makulilo@out.ac.tz

[37] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 304 – 305.
[38] For a detailed discussion about cryptography as well as the public and private keys, see *Electronic Signatures in Law*, 317 – 325.