IN THE HIGH COURT OF TANZANIA

(COMMERCIAL DIVISION)

AT DAR ES SALAAM

COMMERCIAL CASE NO.10 OF 2008

1. LAZARUS MIRISHO MAFIE ..... 1ST PLAINTIFF
2. M/S SHIDOLYA TOURS & SAFARIS ..... 2ND PLAINTIFF

VERSUS

ODILO GASPER KILENGA Alias MOISO GASPER ..... DEFENDANT

Date of last order: 27.05.2010

Date of final submissions: 30.07.2010

Date of ruling: 01.10.2010

RULING

MAKARAMBA, J.:

This is a ruling on a preliminary objection on a point of law the Defendant's Counsel, Mr. Albert Msando raised in this Court on the 27th day of May 2010 in the course of hearing of this suit that some e-mail the Plaintiffs' Counsel sought to tender in evidence through the 1st Plaintiff was inadmissible. On that day, the Plaintiffs Counsel, Senior Counsel Mahatane, while leading the 1st Plaintiff (PW1) in testimony in chief, sought to tender in evidence e-mail containing statements the 1st Plaintiff claim the Defendant made and which the 1st Plaintiff allege to be defamatory. Following the objection, this Court, after hearing brief oral submissions

from Counsel, directed them to conduct further research on the issue of admissibility in evidence of electronically stored information in civil proceedings and address this Court accordingly, a task they carried out with great zeal and industry for which this Court highly commend them. Their submissions and cited authorities in not a small measure have contributed towards the preparation of this ruling.

Before I traverse the arguments of the learned Counsel on the preliminary point of objection, a brief background to the matter is apposite. Central to the preliminary objection are statements in an e-mail the Plaintiffs claim the Defendant sent to the Financial Manager of ***Rockjumper Biriding Tours of Worldwide Birding Adventure*** of South Africa on the 26th day of June 2008, informing that Manager that in the year 2007 the said South Africa tour company had made double payments to the Plaintiffs. The Plaintiffs allege further that in the said e-mail text the Defendant demanded a reward for revealing the fact about the alleged double payments to the South African Tour Company, and further that the Defendant had asked the South African Tour Company not to reveal the Defendant's name to the Plaintiffs' company as this may cost the Defendant, who was an employee of the Plaintiff's company, his job. The 2nd Plaintiff maintains further that anyone reading that e-mail text will inevitably understand that the 2nd Plaintiff and its Managing Director as well as that Managing Director personally knew of the entries of the double payments, and that the said Plaintiffs had deliberately kept quiet about that information with the view to retain excess payments, and further that the Plaintiff would punish any of its employee who would reveal the double

payments to ***Rockjumper Birding Tours*** company. By necessary implication, the Plaintiff allege further, the Defendant called the Plaintiffs dishonest persons and thieves who wantonly steal from clients, something the Plaintiff claim that it is all false. The Plaintiffs further allege that the Defendant published the said false e-mail statement to one KAREN ERASMUS and also to one ADAM in South Africa, as a result of which the Plaintiffs claim to have suffered a great deal of damage not only to their personal reputation and character but also to their tourist business generally. The Plaintiffs' claim against the Defendant is for certain sums of monies as special and general damages resulting from the alleged defamatory e-mail statement which the Plaintiffs claim was sent, made and published by the Defendant. It is the admissibility of the alleged defamatory e-mail statement which the preliminary objection the Defendant's Counsel raised concerns. The main contention of the Defendant's Counsel is that the e-mail containing the alleged defamatory statements being part of electronic evidence is not admissible in evidence in civil proceedings and should therefore be rejected.

The point of law involved in the preliminary objection is that an e-mail being part of electronic evidence is not admissible in civil proceedings. This point of law is a novel one as it has not been dealt with previously by our courts. As rightly submitted by the Defendant's Counsel, the admissibility of electronic evidence in civil proceedings is not yet part of our laws. A novel legal issue as it is obviously creates some challenges to courts which necessarily call for judicial innovation as it holds a stake in the development of the law in so far as the admissibility of electronic evidence

in civil proceedings is concerned. This is the reason why this Court requested Counsel for the parties to address it on the subject in order to come up with a meaningful decision, which may set a direction for course of action in the future.

The e-mail the Plaintiffs sought to be admitted as evidence to support their claim is central to the preliminary objection. This Court however is being called upon to consider the admissibility of electronic evidence in civil proceedings generally, which admittedly is not yet covered under our laws of evidence or civil procedure. There is however some limited sphere in admissibility of electronic evidence in certain specified matters in civil proceedings as well as in criminal proceedings. This Court therefore in dealing with the matter before is doing so without the benefit of any express enactment on admissibility of electronic evidence generally in other civil proceedings, and without any precedent from our courts on admissibility of e-mail to fall back on.

In the course of their submissions, the learned Counsel for the parties have brought into the fore what in my view seems to be two schools of thought on the matter before this Court. The first school of thought is that of "***timid souls***" shared by the Defendant's Counsel and the other school is that of "***bold sprits***" shared by the Plaintiff's Counsel.

The Defendant's Counsel has framed a broad issue ***whether or not electronic documents/records may be admitted as evidence in proceedings of civil nature.*** This issue does not lend itself easily of any quick and straightforward answer. It must be appreciated however, that in this country, aside from certain restrictive amendments to the law of

evidence, and the decision of this Court in the case of **THE TRUST BANK OF TANZANIA VS LE-MARSH ENTERPSRISES LTD. AND TWO OTHERS, Commercial Case No.4 of 2000** (unreported), which dealt with the issue "*whether or not a computer print-out is a banker's book under the Evidence Act, 1967*, there is dearth of statutory provisions and case law on admissibility of electronic evidence in civil proceedings generally.

The first task of this Court however is to examine the existing provisions in our law on admissibility of documentary evidence an d construe them broadly if possible in order to establish a set of rules to guide admissibility of electronically stored information generated for use in court of law as evidence in civil proceedings. The Defendant's Counsel in his submissions mentioned the amendment to the Evidence Act, 1967, brought about by the *Written Laws (Miscellaneous Amendments) (No.2) Act of 2006]*, dealing with what the Plaintiffs' Counsel see to be a "restrictive approach" as it concerned itself only with electronic evidence and records in the banking business under the Banker's Books in the Evidence Act, 1967. This approach, restrictive as it is, in the Plaintiffs' Counsel opinion was most probably ushered in as a result of judicial advice His Lordship Justice Nsekela of the High Court of Tanzania (as he then was) gave in **THE TRUST BANK OF TANZANIA VS LE-MARSH ENTERPSRISES LTD AND TWO OTHERS. Commercial Case No.4 of 2000** (unreported), a case which the Defendant' also cited in his main submissions. The Plaintiffs' Counsel on his part however, went further to explore a subsequent amendment to the *Evidence Act*, 1967 brought about by the *Written Laws (Miscellaneous Amendments) Act [Act No.15 of 2007],*

amending section 40 of the Evidence Act, 1967 by adding section 40A relating to "*admissibility of electronic evidence in criminal proceedings*", which he contends that the Defendant's Counsel overlooked in his submissions. The Defendant's Counsel however annexed to his submissions the *Written Laws (Miscellaneous Amendments) (No.2) Act* [Act No.15 of 2007] which amended section 40 of the Evidence Act, 1967 by adding section 40A which provides as follows:

> *"40A. In criminal proceedings-*
> *(a) An information retrieved from computer systems, networks or servers; or*
> *(b) The records through surveillance of means of presentations of information including facsimile machines, electronic transmission and communication facilities.*
> *(c) The audio or video recording of acts or behavior or conversation of persons charged*
> ***Shall be admissible in evidence.*** *" (emphasis supplied by Plaintiff's Counsel).*

The argument by the Defendant's Counsel that the 2006 amendment to the Evidence Act, 1967 effected through the *Written Laws (Miscellaneous Amendments) Act [Act No.2 of 2006]* is confined only to electronic records in relation to the banking business is also shared by the Plaintiffs' Counsel. However, even after the most current amendment to the Tanzania Evidence Act, 1967 (which is the 2007 amendment), the Defendant's Counsel contend that the Evidence Act, 1967 still does not provide for the admissibility or the receiving in evidence in civil proceedings of electronic records including e-mails except in the course of banking business. The further argument by the Defendant's Counsel is that even

with that, it is only upon meeting the criteria set out in the new section 78A(1) inserted by section 36 of the Amending Act No. 2/2006, which provides as follows:

> *"36. The principal Act is amended by adding immediately after section 78 the following new section –*
>
> *"78A.-(1) a print out of any entry in the books of a bank on micro-film, computer, information system, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, and when such print out is supported by a proof stipulated under subsection (2) of section 78 that it was made in the usual and ordinary course of business, and that the book is in the custody of the bank, it shall be received in evidence under this Act." (the emphasis is of the Defendant's Counsel).*

The Defendant's Counsel having submitted on the shortcomings in the existing law on the admissibility of electronic evidence in civil proceedings, proceeded to explore case law on the subject. The Defendant's Counsel managed to unearth so far the only case decided by our courts which is closer to the situation at hand, that of **THE TRUST BANK OF TANZANIA VS LE-MARSH ENTERPSRISES LTD AND TWO OTHERS. Commercial Case No.4 of 2000** (unreported), where the Commercial Division of the High Court of Tanzania dealt with the issue "*whether or not a computer print-out is a banker's book under the Evidence Act, 1967.*" The Defendant's Counsel however distinguished this case with the issues at hand and submitted that they do not bear any similarity. The Defendant's Counsel however, appreciated the approach His

Lordship Nsekela adopted in that case, who oblivious of the fact that the Tanzania Evidence Act by then was silent on the issue dealt with in the case before him, commented that "*the law must keep abreast of technological changes as they affect the way of doing business.*" The Defendant's Counsel very strongly maintained however that in that case His Lordship Justice Nsekela still confined himself to technological changes that affect the banking industry, and remarked obiter that, "I*t would have been much better if the position were clarified beyond all doubt by legislation rather than judicial intervention.*" As it turned out, the Defendant's Counsel further argued, the legislature in 2006 heeded to the judicial call by His Lordship Nsekela and effected the necessary amendments to the Evidence Act, 1967 to provide for admissibility of computer print-out in evidence as part of banker's books.

The ruling of this Court in that case, as the Defendant's Counsel correctly submitted, and the subsequent amendment to the Evidence Act, 1967 only cured the particular issue of admissibility of electronic records in relation to the banking business, but not in all other scenarios of admissibility of electronic evidence in civil proceedings. It seems to me however that both learned Counsel for the parties share the same sentiments on the role of our courts, which is not to develop a new area of the law of evidence. The Plaintiffs' Counsel however is of the opinion that courts should see to it indeed if there is any legal logic why our law provides expressly on admissibility in evidence of computer print-outs in relation to the banking business and in criminal proceedings, but is silent in relation to admissibility of electronic evidence in other civil proceedings.

The Plaintiff's Counsel wondered if this does not amount to creating an absurdity, which in any event needs to be cured by courts, suggesting that it is within the boundaries of the wisdom of the Court to extend the same terms and conditions to civil proceedings for admissibility of electronic evidence as in criminal proceedings, where the burden of proof is on a ***balance of probabilities,*** a much lighter burden than in criminal proceedings where it is ***beyond any reasonable doubt***. In buttressing further his point the Plaintiffs' Counsel argued that if the legislature has already enacted a law to admit electronic evidence in criminal matters, where the burden of proof is much higher than in civil proceedings, then it will be within the boundaries of its wisdom if this Court extends to civil proceedings the same terms and conditions for admissibility of electronic evidence as for criminal proceedings. In the considered opinion of the Plaintiffs' Counsel, the Court will not be laying down for the first time a new rule as the Defendant's Counsel asserts, but it will be only ***extending*** to civil proceedings "*that which the legislature has already done in respect of criminal proceedings.*" Otherwise there is no legal logic, in the opinion of the Plaintiffs' Counsel, why the legislature did not include the admissibility of electronic evidence in civil proceedings in section 33 of the *Written Laws (Miscellaneous Amendments) Act [Act No.15 of 2007*, an absurd lacunae unreasonably left by the legislature, which is imperative for the Courts to plug given the overwhelming and universal use of computers, e-mails, electronic storage of information, electronic print-out etc., the Plaintiffs' Counsel very happily and confidently surmised.

In his bid to show that under the existing law the admittance of electronic evidence in civil proceedings is still a raw issue posing unanswered questions not only in our courts but also in courts in other jurisdictions in countries endowed with more technologically advanced legal systems than ours, the Defendant's Counsel in his submission travelled as far as to the United States District Court for the District of Maryland, where through web search managed to unearth an article discussing a legal opinion rendered by Hon. Paul W. Grimm, Chief United States Magistrate in May 2007 in the case of **JACK R. LORAINE AND BEVERLY MACK VS. MARKEL AMERICAN INSURANCE COMPANY Civil Action No.PWG-06-1893.** The Defendant's Counsel however could not provide this Court with a full report of that case. In its efforts to get to the substance of the said opinion this Court managed to uncover the web report of that case at http://indianalawblog.com/documents/Lorraine_v_Markel.pdf, which is a 101 page "***MEMORANDUM OPINION***" handed down by Judge Grim. This case although it dealt with arbitration matters it involved an issue of admissibility of e-mail in evidence, which is similar to the issue we are dealing with presently. In that case Judge Grim however dismissed both parties' motions without prejudice for their failure to properly establish the ***authenticity of e-mail documentation as evidence to support their case.*** Judge Grim however, seized the occasion to put together a comprehensive opinion on the evidentiary hurdles to be overcome in getting electronically stored information into evidence in a court of law. According to Judge Grim, it is critical for Counsel to be p*repared to* recognize and appropriately deal with the evidentiary issues associated

with admissibility of electronically stored information. In that case, Judge Grim also realized that in the United States of America cases abound regarding the discoverability of electronic records, but there is lack of comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence.

As I intimated to earlier, the task of this Court is to analyze and broadly construe the existing laws in order to establish court rules on admissibility of electronic evidence in civil proceedings. In the considered opinion of the Defendant's Counsel, given the absence of any express authority in statutory provisions in an Act of Parliament or precedent, the present case is not one of those situations where a court may lay down a rule for the first time. The Defendant's Counsel argued further that there is so much at stake involved if electronic records are received in evidence in civil proceedings without there being in place acceptable rules and procedures for their admissibility. The Plaintiffs' Counsel much as he seems in a way to appreciate the view by the Defendant's Counsel on the stakes involved in admitting in evidence electronically stored information in civil proceedings, which stakes although the Defendant's Counsel referred to them without any further elaboration, they relate particularly to other primary rules of evidence such as the rules on hearsay, rules of authenticity; identity of the author of the document or information etc.

The Plaintiff's Counsel however, is of the strong view that the present case is a fit one for the courts to lead the way by filling the lacunae in the existing laws on admissibility of electronic evidence in civil proceedings by extending to civil proceedings that "*which the legislature has already done*

in respect of criminal proceedings." The Defendant's Counsel on his part however, seems to entertain a totally different view. Picking a leaf of advice from Fitzgerald, *Salmond on Jurisprudence* (12th Edition)(1966) reproduced in *Introduction to the Legal Systems of East Africa*, the Defendant's Counsel is of the strong view that if this Court feels inclined to develop this particular area of the law, the rules to be applicable in the present case should be those found in the existing law under the Evidence Act, 1967 [Cap.6 R.E. 2002]. The Defendant's Counsel further insisted that the e-mail statements intended to be tendered in evidence by the Plaintiffs in this suit should not be admitted, but the Court may proceed "*to set down new rules for establishing the validity of electronic documentation, or electronically stored information in view of the growth in the creation, storage and sharing of documents electronically.*" The Defendant's Counsel however, wonders whether our Courts are well equipped to handle electronic evidence in view of absence of rules and procedures for the admissibility of such evidence. The Defendant's Counsel is also worried if our courts, in the absence of any express statutory enactment, can take the bold leap and exercise their powers to mould the law by taking into account technological advancements. The Defendant's Counsel insisted that there has to be specific rules and procedures enacted by the legislature to be followed by courts in admitting electronic evidence. The Defendant's Counsel cited some examples from other jurisdictions including Kenya, the United States of America, the Philippines and the United Kingdom where such rules already exist. The Defendant's Counsel attached to his submissions a web article by Cathy Mputhia titled "***When Digital***

Evidence is Admissible in Court" where the learned author discusses some provisions in the Kenyan Evidence Act particularly section 65 which allows the admittance of computer print outs for use in trial and section 65(6) which provides for standard of authentication needed before electronic evidence can be admitted.

The Defendant's Counsel argues one of the most critical issues courts will be faced with in relation to admitting in evidence electronic evidence such as e-mail is its authenticity. According to the Defendant's Counsel any person can easily log into someone's e-mail account and create documents, even bearing a company's letter head and the president's signature. The Defendant's Counsel insisted that the Tanzania Evidence Act, 1967 does not provide for the admissibility of electronic records and there are no standards or rules set for the admissibility of such evidence in our law. The Defendant's Counsel argued further that the Plaintiffs have not even on their own motion before filing the suit or before tendering the alleged emails in evidence, tried to establish and adhere to the standards followed in other jurisdictions so that issues such as hearsay, authenticity, relevancy, unfair prejudice, and whether the emails are original documents or duplicates would not arise.

The Commercial Division of the High Court of Tanzania in **Commercial Case No.4 of 2000** between **TRUST BANK TANZANIA LTD AND LE-MARSH ENTERPRISES LTD**, (unreported) has already developed the law by recognizing computer print outs as evidence, which is now part of our law following amendments done to the Evidence Act. The issue in that case was *whether or not a computer print-out is a banker's book under the*

Evidence Act, 1967. In that case issues of hearsay, authenticity, relevancy, unfair prejudice, and whether the emails are original documents or duplicates did not arise and there are no standards which were set by the court in that regard. The two amendments to the Evidence Act did not touch on the issue of authenticity either. There is therefore lack of set standards in that regard in our law. His Lordship Justice Nsekela in that case having cited with approval section 5 of the ***English Civil Evidence Act*** of 1968 on admissibility of statements produced by computers, took a very bold step of allowing in evidence a computer print-out as part of a banker's book in the Evidence Act, 1967. Section 5 of the English Civil Evidence Act, 1968 in addition to widening the admissibility of hearsay evidence in documents produced by a computer, also made specific provision for computers. It is worth noting however, that in England, the Civil Evidence Act of 1995 has greatly simplified and relaxed the law as found in the English Civil Evidence of 1968, by encompassed electronic documents without mentioning either "*documents*" or "*computers*", under its section 13 which stipulates that:-

> *"13. In this Act–*
>
> ...
>
> *"document" means anything in which information of any description is recorded, and "copy", in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly;"*

Furthermore, currently in England, the substantive provisions in the English Civil Evidence Act of 1995 allow the admission of copies of any degree of remoteness from the original by providing as follows:-

> *"8.--(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved–*
> *(a) by the production of that document, or*
> *(b)* ***whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve.***
> *(2)* ***It is immaterial for this purpose how many removes there are between a copy and the original.***
>
> *9.--(1)* ***A document which is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.***
> *(2) A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong.*
> *For this purpose--*
> *(a) a document purporting to be a certificate signed by an officer of a business or public authority shall be deemed to have been duly given by such an officer and signed by him; and*
> *(b) a certificate shall be treated as signed by a person if it purports to bear a facsimile of his signature.*
> *(3) The absence of an entry in the records of a business or public authority may be proved in civil proceedings by affidavit of an officer of the business or authority to which the records belong.*
> *(4) In this section–*
> *"records" means records in whatever form;*
> *"business" includes any activity regularly carried on over a period of time, whether for profit or not, by anybody (whether corporate or not) or by an individual;*

"officer" includes any person occupying a responsible position in relation to the relevant activities of the business or public authority or in relation to its records; and
"public authority" includes any public or statutory undertaking, any government department and any person holding office under Her Majesty.
(5) The court may, having regard to the circumstances of the case, direct that all or any of the above provisions of this section do not apply in relation to a particular document or record, or description of documents or records."

The English law which His Lordship Nsekela cited in **Commercial Case No.4 of 2000 between TRUST BANK TANZANIA LTD AND LE-MARSH ENTERPRISES LTD,** unreported) has since undergone some further development in England as evidenced by the provisions of the English Civil Evidence Act of 1995, which I have cited above. Although this case has yet to be affirmed or reversed by the highest court of the land, the Court of Appeal of Tanzania, it forms an illuminating example of how a court can can embark on what has come to be popularly known as judge-made law. It is encouraging to note however, that following the decision of Justice Nsekela, the legislature in Tanzania embarked, albeit on a piecemeal basis, on a course of amending the Tanzania Evidence Act, first in 2006, vide the *Written Laws (Miscellaneous Amendments) Act [Act No.2 of 2006]* by allowing in evidence in civil proceedings "*a print out of any entry in the books of a bank*", and through the *Written Laws (Miscellaneous Amendments) Act [Act No.15 of 2007*] by allowing in evidence "*an information retrieved from computer systems, networks or servers*" among others, in criminal proceedings. Despite this piece meal approach to legislating, the law on admissibility of electronic evidence in Tanzania is still

highly unsatisfactory. The main task for this Court presently is therefore to develop the law a step further by setting out guiding standards for recognizing admissibility of electronically stored evidence in civil proceedings. It is worth noting that this Court in **Commercial Case No.4 of 2000 between TRUST BANK TANZANIA LTD AND LE-MARSH ENTERPRISES LTD,** unreported) has already established judicially that a computer print-out is a bankers book under the Evidence Act, 1967, which has now been legislated and therefore part of our law. In that case, this Court embarked on a journey of statutory interpretation by appreciating first that the term "*bankers book*" was not defined anywhere in the Evidence Act, 1967. Different however from the present case the term "document" is already defined in the Evidence Act, 1967. The first task for this Court is therefore to establish whether a computer print-out of statements contained in an e-mail is a document in the context of our law of evidence.

The learned author Tania Correia, a Legal Consultant in a web article titled "***Legal Admissibility of Documentary Evidence in Civil and Criminal Proceedings***" (downloaded on 27/09/2010 at http://www.ssrltd.com/WhitePapers/Legal%20Admissibility%20of%20Documentary%20Evidence%20in%20Civil%20and%20Criminal%20Proceedings.pdf), gives some quite insightful thoughts on the meaning of the term "*document*" and makes a distinction between admissibility and weight of evidence. In the said article, the learned author kicks off the discussion by citing a very old English case of **R. V. DAYE (1908) 77LJK8 659** where it was stated that:

"There is a document whenever there is writing or printing capable of being read, no matter what the material may be upon which it is impressed or inscribed."

According to the above illustration, documents cover any record of evidence or information and are not limited to pieces of paper. In terms of section 3 of the Tanzania Evidence Act, 1967 [Cap.6 R.E. 2002], a "*document*" means:

> *"any **writing**, handwriting, typewriting, printing, photostat, photograph and **every recording upon any tangible thing**. **any form of 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; (the emphasis is of this Court).*

And according to section 4 of the *Interpretation of Laws Act* [Cap.1 R.E. 2002], a "document":

> *"includes any publication and any matter written, expressed, or described upon any substance by means of letters, figures, or marks, or **by more than one of those means**, which is intended to be used or may be used for the purpose of recording that matter..."*

It is interesting to note however, that whilst the form of words may have changed over the years, the description of a "*document*" given in the old English case of **R. V. DAYE (1908) 77 LJK8 659** (supra) has not really changed over the decades. Our Evidence Act, 1967 which we received by way of India was promulgated in 1875, long before documents Bridge L.J.

referred to at page 82 of **BARKER V. WILSON [1980] 2 All E.R. 80**, cited in **Commercial Case No.4 of 2000 between TRUST BANK TANZANIA LTD AND LE-MARSH ENTERPRISES LTD,** (unreported), as "*made by any of the methods which modern technology makes available*", had come into existence. An e-mail form part of documents made by modern technology. Contrary to the view entertained by the Defendant's Counsel that the business of creating a rule on admissibility of electronically stored information such as an e-mail should be left to the legislature since this kind of rule has not been done before, I am alive to the words of Lord Denning in **PACKER V PACKER [1954] P 15** that:

> "*...If we never do anything which has never been done before, we shall not get anywhere. The law will stand still whilst the rest of the world goes on: and that will be bad for both.*"

In the present case, the duty of this Court is to "*construe*" the words in the existing laws and then to "*extend*" that construction to cover electronically stored information. The idea is not as the Plaintiffs' Counsel would wish this Court to do to extend to civil proceedings rules on admissibility of electronic evidence developed for criminal proceedings, but to construe the term "*document*" in section 3 of the Tanzania Evidence Act, 1967 [Cap.6 R.E. 2002] to encompass an e-mail for purposes of admissibility in civil proceedings. In so doing, this Court will be fulfilling one of its basic and noble duties under the Article 107A of the Constitution of Tanzania as the last arbiter of rights and custodian of the laws. As was appreciated by the highest court of the land in **TANZANIA COTTON**

MARKETING BOARD VS CORGECOT COTTON COMPANY SA [1997] TLR 165

while construing the words "*registered post*" in Rule 4 of the Arbitration Rules, 1957:

> "*...the words registered post should be interpreted widely enough to take into account the* ***current development in communication technology*** *that has taken place since 1957 when the rules were enacted. It is common knowledge that since that time other modes of postage have been introduced." (the emphasis is of this Court).*

In that case, the DHL courier services which were not in existence in 1957 when the postage rule in the Arbitration Rules was promulgated, was considered to be a modern mode of postage and thus falling within the words "*registered post*" in Rule 4 of the Arbitration Rules, 1957. In 1875 when the Indian Evidence Act from which our current Evidence Act, 1967 derives was promulgated, the modern methods of making e-mail by computers were not yet in existence. This Court however, given technological revolution in information communication which has been sweeping the world since the last century, cannot afford to hide behind old ways of communicating by refusing to accept other types of electronic documents such e-mail, which may carry electronic information capable of being stored on computers and generated by being printed out. It is for this reason that this Court feels very strongly that to extend the definition of a "*document*" under section 3 of the Evidence Act by interpreting it broadly to cover evidence generated by computers including e-mail subject of course to the general evidentiary rules on documentary evidence found in Part III of the Evidence Act, [Cap.6 R.E. 2002].

According to section 3 of the Evidence Act, 1967 the term "*document*" includes among other things "*writing*", "*every recording upon any tangible thing*" and "*any form of communication, which may be used for the purpose of recording any matter*" provided that "*such recording is reasonably permanent and readable by sight.*" An e-mail is also a writing containing electronically recorded information. The only difference between paper documents and electronic documents however, is that, whereas the former is "reasonably permanent" and readable by sight, the latter may not be reasonably permanent although it is readable by sight. This is where the requirement fort authentication comes in. An e-mail being an electronically produced document forms part of computer records capable of being retrieved from a computer database containing relevant information. The need for authentication also comes in particularly in terms of need to prove reliability of the equipment and mode of entering data. An e-mail being an "electronically produced *document*" within the meaning assigned to that term under section 3 of the Evidence Act, 1967, in my view much as issues about its admissibility in evidence in civil litigation may arise, the standards to be set by courts as to authentication go more to the weight to be attached by this Court to the e-mail in the event it is admitted in evidfence.

The existing rules in our law of evidence on admissibility of documents in my view suffice to cover electronically generated information without requiring the intervention of Parliament. The only thing which is missing are standards for determining authenticity. As for standards on relevancy and hearsay, the existing rules of evidence suffice. The rules to be developed by courts are for setting out prior requirements to be met

before an electronically generated document can be admitted in evidence in civil proceedings. This is where opinion given by Judge Grim in **JACK R. LORAINE AND BEVERLY MACK VS. MARKEL AMERICAN INSURANCE COMPANY Civil Action No.PWG-06-1893** becomes relevant.

As the Defendant's Counsel correctly argued the fact that the weight of an e-mail being a computer generated record as evidence may be reduced unless there is sufficient authentication to convince the court that it is an accurate copy is highly critical. ***Authentication is proving to the court that a document is what it purports to be.*** In the present case, the Plaintiffs have to prove that the original of the e-mail sought to be tendered in evidence is authentic and also that the e-mail has not been altered since the date it was retrieved from the computer. As the learned author in "***Legal Admissibility of Documentary Evidence in Civil and Criminal Proceedings" (supra) argues*** such authentication evidence would normally be in the form of an "*audit trail*" that is, ***showing how the original document (e-mail) was turned into an electronic image stored in the computer system from where it was retrieved and then produced to the court.*** If an audit trail like this cannot be produced, the electronic evidence may be rejected.

The content of the e-mail document could also be an issue. In civil proceedings there is unlikely to be any problems about producing copies of the various e-mail documents (either electronic or as a hard copy), except in some fraud actions, where this may not be the case for example, if a signature is at issue then it is obviously better to produce the original document rather than an electronic image or even a photocopy of it. In the

present case arguments over the admissibility of the e-mail as electronically generated evidence can lead to investigations into the computer system which produced the paper on which the e-mail statements is produced, the method of its storage, operation and access control, and even to the computer programmes and source code used. It may also be necessary for the Plaintiffs to satisfy this Court that the information on the e-mail was stored in a "proper" manner.

The Defendant's Counsel has advanced arguments questioning the authenticity of the disputed e-mail which in my view is a tactic to discredit the e-mail as piece of evidence and make it inadmissible. It is therefore very important that the Plaintiffs seeking to use the electronic information on the e-mail in this Court to have an ***audit trail***. The issues relating to authenticity which the Defendant's Counsel has raised in relation to computer generated records, in my view would not have been a problem in these proceedings if the Plaintiffs had disclosed the evidence through the process of discovery, where the documents in the possession, power and control of the parties relating to the issues in dispute would have been exchanged. In the present case, the process of discovery did not take place. The Plaintiffs simply annexed the disputed e-mail to the Plaint. It is common practice for parties in a civil suit to provide and exchange a list of documents and as such a document which is asserted on the list to be a copy is presumed to be a true copy unless its authenticity is specifically disputed by the other party. If, however, the admissibility of the document is being disputed as is the case presently, evidence as to its authenticity will be required. In criminal proceedings, however, where the burden of

proof is much higher than in civil proceedings, it will always be necessary for the party seeking admissibility of a particular document to be able to produce some founding testimony as to the source and authenticity of the document, especially if it is an image, otherwise the courts may refuse to admit the evidence. I presume this is the reason why the legislature in Tanzania provided specifically for the admissibility of "***computer records***" in criminal proceedings vide the ***Written Laws (Miscellaneous Amendment) Act, No.15 of 2007,*** the Plaintiffs' Counsel alluded to in his submissions. It is the discretion of this Court properly directing its mind on the relevant law, to always to exclude evidence which has doubtful value. In criminal proceedings a prosecutor or party to civil litigation will always need to be prepared to offer further evidence about the source of electronic evidence and the processing and storage it has undergone since it was first recorded. As it was held in one English case, that of **R.V. ROBSON and HARRIS [1972] 1W.L.R. 651**), "*a person producing a recording as evidence must describe its provenance and history so as to satisfy the judge that there is a prima facie case that the evidence is authentic.*" In the present case the Plaintiffs have not been able to cross the hurdle of proving the authenticity of the e-mail they are seeking to produce in evidence. Our Evidence Act, 1967 however does not contain any express provision on authentication and identification of electronically stored information as is the case with the Kenyan Evidence Act or the United States Federal Rules of Evidence. The underlying concept under the Evidence Act, 1967 is relevancy of evidence to the facts in issue. In relation to electronic evidence a party seeking it to be admitted in evidence has to

lead evidence sufficient to support a finding that the matter in question is what its proponent claims. Authentication of electronically stored information may require greater scrutiny than that required for the authentication of "*hard copy*" documents but this does not mean abandoning the existing rules of evidence when doing so. In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If however, a computer processes data rather than merely storing it, as is the case presently where there is a computer print out of e-mail statements, authentication issues may arise.

In **JACK R. LORAINE AND BEVERLY MACK VS. MARKEL AMERICAN INSURANCE COMPANY Civil Action No.PWG-06-1893,** Judge Grim revisited the relevant rules in the US Federal Rules on Evidence and made the following observation:

> *"Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states:*
> *(b) Illustrations.*
> *By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:*
> *(1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.*
> *(2) Non-expert opinion on handwriting. Non-expert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.*

(3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.

(4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) Ancient documents or data compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority."

According to Judge Grim, the ten methods identified by Rule 901(b) of the US Federal Rules of Evidence are non-exclusive citing the FEDERAL

RULES ON EVIDENCE 901(b) Advisory Committee's has noted that "*The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.*"; also citing WEINSTEIN at §901.03[1] that "*Parties may use any of the methods listed in Rule 901(b), any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be.*"

Judge Grim having revisited the relevant rules in the US Federal Rules of Evidence on electronically stored information (ESI) remarked that "*there is no form of ESI more ubiquitous than e-mail.*" As was in that case, it is the category of ESI at issue in the present case. According to Judge Grim:

> "*Although courts today have more or less resigned themselves to the fact that "[w]e live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world, ...Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence provided the following guidance in establishing the authenticity of electronically stored information:*"

Judge Grim recognizing that not surprisingly, there are many ways in which e-mail evidence may be authenticated proceeded to state that one well respected commentator has observed:

"[E]-mail messages may be authenticated by direct or circumstantial evidence. An email message's distinctive characteristics, including its "contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances" may be sufficient for authentication.

Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender's listed e-mail address.

The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message. E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness."

Rule 901(b)(4) of the US Federal Rules of Evidence is one of the most frequently used by Courts in the United States of America to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by "[*appearance, contents, substance, internal*

patterns, or other distinctive characteristics, taken in conjunction with circumstances." Courts in the United States of America have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites [See ***United States v. Siddiqui***, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (*allowing the authentication of an e-mail entirely by circumstantial evidence, including the presence of the defendant's work e-mail address, content of which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail*). Rule 901(b)(9) of the US Federal Rules of Evidence recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by "*evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.*" In addition to the non-exclusive methods of authentication identified in Rule 901(b), Rule 902 of the US Federal Rules of Evidence identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence, commonly referred to as "self-authentication."

Judge Grim discussed in detail the five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit, nameiy:

(1) ***Relevance***

The first evidentiary hurdle to overcome in establishing the admissibility of ESI is to demonstrate that it is relevant, as defined by Evidence Act,

[Cap.6 R.E. 2002] as amended. "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. It is important therefore for the proponent of the evidence to have considered all of the potential purposes for which it is offered, and to be prepared to articulate them to the court if the evidence is challenged.

(2) Authenticity

The party seeking an ESI to be admitted in evidence must provide authenticating facts for the e-mail and other evidence that the party wish to proffer in support of its case but not simply to attach the exhibits. Absence of authentication strips the e-mails of any evidentiary value because this Court can not consider them as evidentiary facts. The Plaintiff has to cure the evidentiary deficiencies. The Plaintiffs' Counsel needs to plan which method or methods of authentication that will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering Counsel needs also to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

(3) The Hearsay Rule

The other hurdle which must be overcome when introducing electronic evidence is the potential application of the hearsay rule. Hearsay issues are pervasive when electronically stored and generated evidence is introduced. According to PAUL R. RICE, ***ELECTRONIC EVIDENCE: LAW AND PRACTICE***, 262 (ABA Publishing 2005):

> *"Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.")*

There are five separate questions that must be answered:

(i) does the evidence constitute a statement;
(ii)was the statement made by a "declarant";
(iii) is the statement being offered to prove the truth of its contents;
(iv) is the statement excluded from the definition of hearsay; and
(v) if the statement is hearsay, is it covered by one of the exceptions to the hearsay rule.

It is critical to conduct a proper hearsay analysis by considering each of the above questions.

The second question that must be answered in the hearsay analysis is that a "*writing*" or "*spoken utterance*" cannot be a "*statement*" under the hearsay rule unless it is made by a "*declarant*", that is, a person who makes a statement. When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as

the "*report*" generated when a fax is sent showing the number to which the fax was sent and the time it was received, or an e-mail print out, there is no "*person*" involved in the creation of the record or the e-mail print out, and no "*assertion*" being made. For that reason, the record or e-mail print out is not a "*statement*" and cannot be hearsay.

The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements." Where the writings are non-assertive, or not made by a "person," courts in the United States have held that they do not constitute hearsay, as they are not "statements" [See ***United States v. Khorozian***, 333 F.3d 498, 506 (3d Cir. 2003)].

The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose. Once it has been determined whether evidence falls into the definition of hearsay because it is a statement, uttered by a declarant, and offered for its substantive truth, the final step in assessing whether it is hearsay is to see if it is excluded from the definition of hearsay. Judge Grim commented that "*given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered*

against that party" citing ***Siddiqui case***, 235 F.3d at 1323 (*ruling that e-mail authored by defendant was not hearsay*).

(4) The original writing rule

When counsel intends to offer electronic evidence at trial he must determine whether the original writing rule is applicable, and if so, the Counsel must be prepared to introduce an original, a duplicate original, or be able to demonstrate that one of the permitted forms of secondary evidence is admissible. In the present case, the Plaintiffs' Counsel did not address the original writing rule, despite its obvious applicability given that the e-mail was closely related to the controlling issue in this suit which is defamatory statements contained in the e–mail which the Plaintiffs allege were published by the Defendants and therefore prove of the contents of the e-mail will be an issue. It has been acknowledged that the original writing rule has particular applicability to electronically prepared or stored writings, recordings or photographs. Judge Grim cited one respected commentator who observed as follows:

> *"Computer-based business records commonly consist of material originally produced in a computer (e.g. business memoranda), data drawn from outside sources and input into the computer (e.g. invoices), or summaries of documents (e.g. statistical runs).*
>
> *The admissibility of computer-based records "to prove the content of a writing" is subject to the best evidence rule... which generally requires the original of a writing when the contents are at issue, except that a "duplicate" is also admissible unless a genuine issue is raised about its authenticity. A duplicate includes a counterpart produced by "electronic re-recording, which accurately reproduces*

*the original." Courts often admit computer-based records without making the distinction between originals and duplicates [*WEINSTEIN at § 900.07[1][d][iv]."

It is apparent that the definition of "*writings, recordings and photographs*" in our Evidence Act includes evidence that is electronically generated and stored. Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form that the information ultimately assumes for useable purposes is words and figures. Hence, the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments. According to Judge Grim, the following are circumstances in which secondary evidence may be introduced instead of the original:

(a) *whether the writing, recording or photograph ever existed in the first place;*

(b) *whether some other writing, recording, or photograph that is offered into evidence is in fact the original; and*

(c) *whether "other" (i.e. secondary) evidence of contents correctly reflects the content of the writing, recording or photograph.*

(5) The need to balance its probative value against the potential for unfair prejudice, or other harm

According to Judge Grim, when a lawyer analyzes the admissibility of electronic evidence, he or she should consider whether it would unfairly

prejudice the party against whom it is offered, confuse or mislead the jury (or assessors in this part of the world), unduly delay the trial of the case, or interject collateral matters into the case. Courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances:

> *(1) When the evidence would contain offensive or highly derogatory language that may provoke an emotional response;*
>
> *(2) When analyzing computer animations, to determine if there is a substantial risk for mistaking them for the actual events in the litigation;*
>
> *(3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs;*
>
> *(4) In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.*

I have endeavoured to outline in greater details the above the five hurdles discussed by Judge Grim which any Counsel seeking to tender in evidence electronically stored information may face. Whether the e-mail as part of electronically stored information (ESI) is admissible into evidence is determined by a collection of five standards as outlined above which present themselves like what Judge Grim referred to as "a series of hurdles to be cleared by the proponent of the evidence." Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible.

The Plaintiffs must therefore consider the following standards rules:

(1) Is the e-mail relevant as determined under the Evidence Act, 1967 [Cap.6 R.E. 2002] (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be);

(2) If relevant under the Evidence Act, 1967 [Cap.6 R.E. 2002] as amended is it authentic in the sense that, can the proponent show that the e-mail is what it purports to be;

(3) if the e-mail is offered for its substantive truth, is it hearsay as defined under the rules in the Evidence Act, [Cap.6 R.E. 2002] as amended and if so, is it covered by an applicable exceptions to the hearsay rules under the Evidence Act, 1967 [Cap.6 R.E. 2002] as amended;

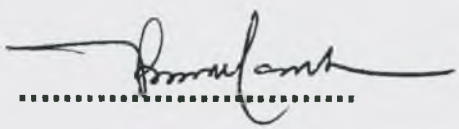
(4) is the e-mail that is being offered as evidence an original or duplicate under the original writing rule, of if not, is there admissible secondary evidence to prove the content of the e-mail; and

(5) Is the probative value of the e-mail substantially outweighed by the danger of unfair prejudice or other identified harm.

I consider the above standards to be the set court rules for guiding this Court in determining the admissibility of electronically stored information (ESI), which is not limited to e-mails only, but may encompass

other forms of electronic evidence such as computer print outs, website messages etc.

Given the pendency by the Plaintiffs' to clear the hurdles in seeking the e-mail to be admitted in evidence using the standards as outlined by this Court above, this Court cannot at this stage and point in time, conclusively determine the preliminary objection. The trial will proceed with the examination in chief of PW1 from where it ended by the Plaintiffs' Counsel clearing the hurdles that present themselves in the five set standards for testing admissibility of electronically stored information as outlined in this ruling. I shall make no order for costs. It is accordingly ordered.



.....

R.V.MAKARAMBA

JUDGE

01/10/2010

Ruling delivered in Chambers this 1st day of October 2010 in the presence of Mr. Lazaro, I., and Mr. Lazaro, Mafie, the Plaintiff in person and in the presence of Mr. Odillo, Gaspar, the Defendant in person and in the absence of their Advocates.

.....

R.V. MAKARAMBA

JUDGE

01/10/2010

Word count: 9,841