Admissibility of email communications in Court proceedings in Uganda

In today's day and age of Information Technology, the nature of human communication has incrementally been modernized and digitized...

KAA
KAMPALA ASSOCIATED ADVOCATES
Celebrating 20 Years

In today's day and age of Information Technology, the nature of human communication has incrementally been modernized and digitized. Unlike in the past, communication in many facets of human life have been carried over the medium of emails. This is not surprising, considering the instantaneous, easy and cheap structure around the use of emails. As with many aspects of human life, many times, email communication is made within the context of non-contentious interactions. As with many things in life, sometimes, the email communication could become evidence in the event of a dispute between the parties, as to what was communicated or agreed upon.

It is very unsettling for people to learn that email, that they thought is strong proof of "Who said what to whom" is easy to defeat. Whereas emails can indeed be admitted as evidence in Court, the reliability of email evidence may become a subject of scrutiny within the Court rules regarding the admissibility and authenticity of evidence. For email communication, burden of proof lies with the party who wishes to employ an email record as evidence of an electronic transaction and therefore such records must be in a court-admissible format.

As with many things within the Information Technology field, anyone who is technology savvy, can easily change the email address, timestamp and message text so the other side can easily claim that you altered the email and printed it off. Printed email is definitely not admissible at court as the other side can simply challenge email's authenticity.

Additionally, it is estimated that approximately about 3% of all non-bulk emails never reach their destination. This means that there is no guarantee that all outgoing emails reach the intended destinations. Even emails with multiple recipients will not necessarily reach all the addresses. The person seeking to rely on the email communication, will therefore have the burden of proving that your important message was not within those emails.

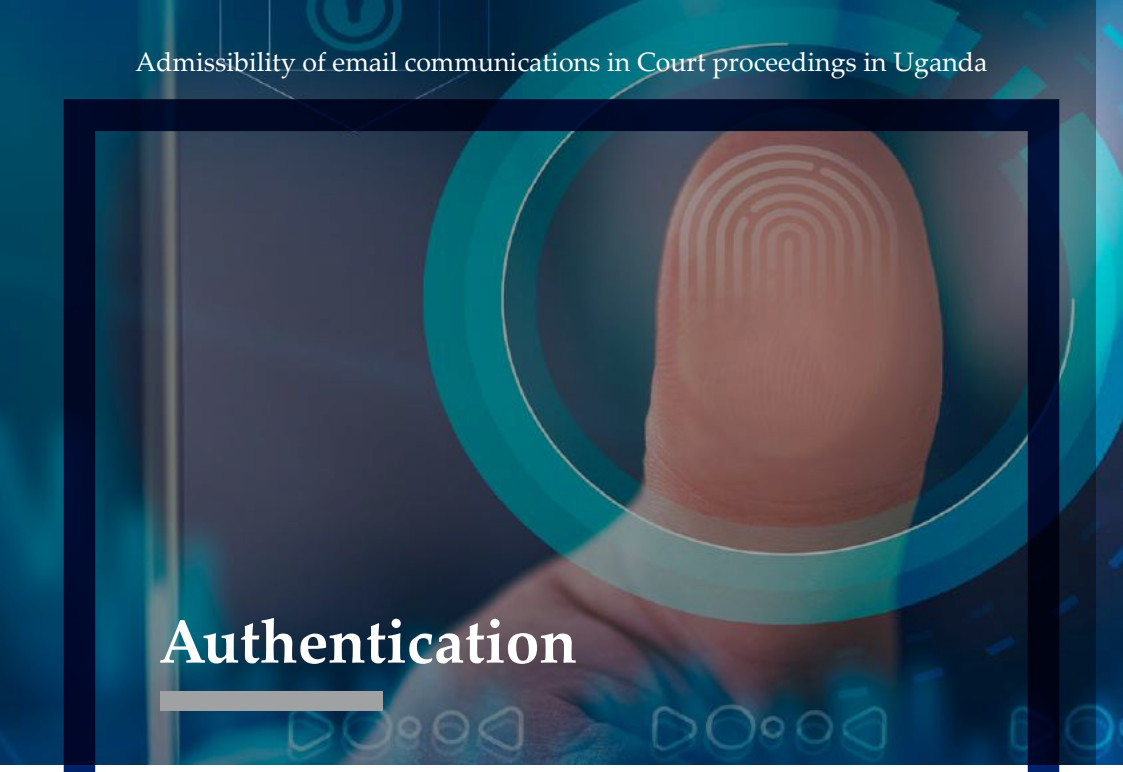
It is therefore imperative to explore and discuss some of the key issues that are important in ensuring that email communication can be admitted in Court as evidence. Ultimately, the question as to whether emails are admissible into evidence will be determined by a collection of evidence rules that present themselves like 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.

Relevance

Like with any other kind of evidence, admitting email evidence generally requires showing that an email is relevant to the case and a specific person authored and/or sent it. There are a variety of different ways to accomplish this, including: through agreement, through company records, and possibly through the email itself.

This is informed by section 4 of the Evidence Act, which provides that subject to any other law, evidence may be given in any suit or proceeding of the existence or nonexistence of every fact in issue, and of such other facts as are hereafter declared to be relevant.

As such, any evidence of email communication that is relevant to the issues on Court can be admitted as relevant evidence.



Authentication

In order to have email evidence admitted at trial, it must be authenticated. This requires the lawyer to lay a proper foundation for the email's authenticity. Section 8 (2) of the Electronic Transactions Act, provides that, a person seeking to introduce a data message or an electronic record in legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.
The test of authenticity is that the proponent must present evidence sufficient to support a finding that the matter in question is what its proponent claims. Authenticity is ordinarily a condition precedent to admissibility

Emails give rise to the difficulty of authenticating their actual author; even if they have been sent from one's email address. This is because it is possible that anyone can send an email from someone else's email address. Additional proof is therefore needed to establish authorship. It is therefore important that any person seeking to rely on the such email evidence, lays a foundation for the admissibility of email messages.

The proponent of such evidence must present some proof that the email message[s] were actually authored by the person who allegedly sent them. There must be evidence that the messages were actually authored by the person alleged to have sent them. This includes admissions by the person who sent them or circumstantial evidence such as testimony by the recipient that they have in the past received email messages from the alleged author from that email address. There could also be something which shows the author wrote the message, such as a personalized signature. The Missouri Court of Appeals, Eastern District in T.R.P v. B. B. , recently (June 2018) confirmed the foundational requirements on the authorship of the message, and highlighted that evidence of authorship can be circumstantial and need not be onerous.

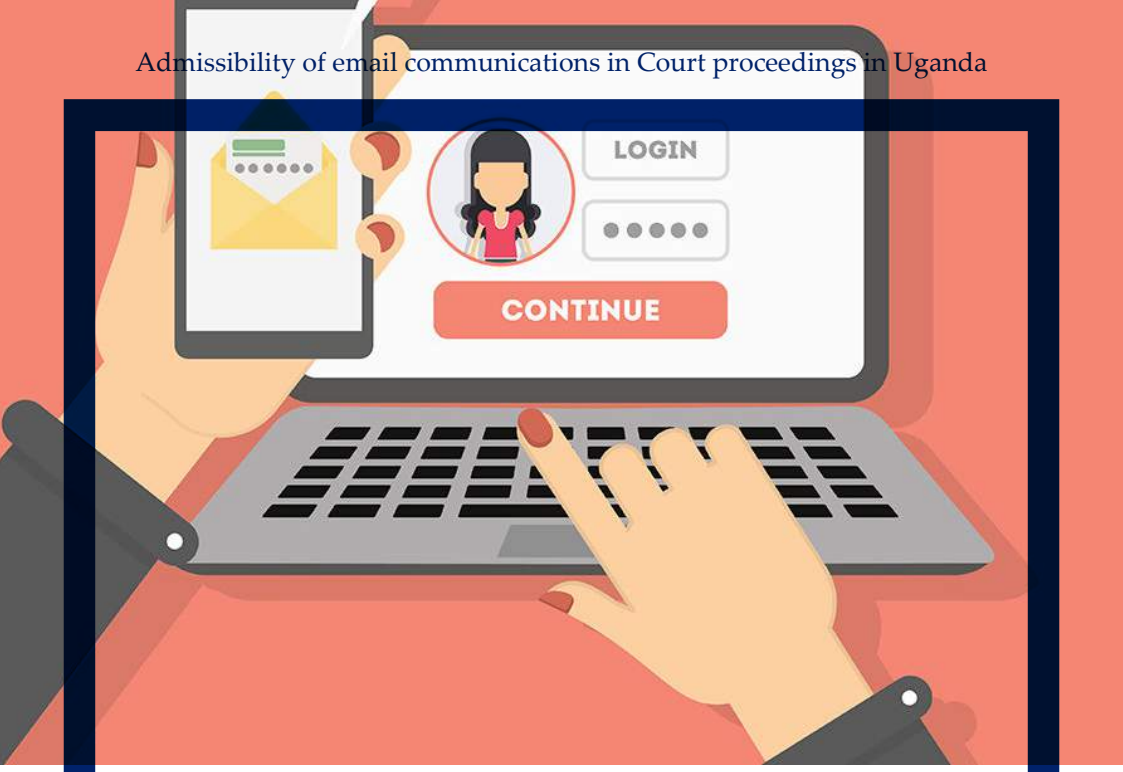
Admissibility

Section 5 of the Electronic Transactions Act, provides for the admissibility of data messages. Section 8 (6) of the Act provides that, for the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of set standards, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

The requirements of admissibility of emails in evidence were laid out by Magistrate Judge, Judge Paul W. Grimm in the United States of America case in Lorraine Vs Markel America Insurance. Co. 2007 WL. The Judge refused to allow either party to offer emails in evidence. He found that they failed to meet any of the standards for admission under the Federal rules of evidence.

In that case, the emails were not authenticated but simply attached to their pleadings as exhibits (as it's the common practice in Ugandan litigation). Even though neither party directly challenged the admissibility of the other's email evidence, the court was not in position to consider emails, because no foundational basis had been provided by the parties for admissibility or authentication. In Judge Grimm's words,

> “Unauthenticated emails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic issues that are highlighted by their electronic medium. Given the pervasiveness today of electronically prepared and stored records as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately del with the evdentiary issues associated with the admissibility of electronically generated and stored evidence”



It is therefore imperative for counsel to take into consideration the need to lay the foundation for the admission of emails while tendering in emails as part oftheir evidence. Whereas, emails have generally been admitted in many case hearings, such have been on account luck rather than establishing the procedure for the admission of emails. It would therefore be possible for an opposing lawyer to object to the admission of emails in future hearings and if properly done, would potentially defeat any application to have such emails tendered in.

Email chains & Hearsay evidence

An e-mail often has attached to it the email or series of emails to which it is responding, creating an email "chain," also known as a "thread." It is important to note that, each distinct email forming part of the email chain is strictly speaking a separate communication, subject to separate authentication and admissibility requirements.

In considering the issue of email chains, it is important to note that most email systems, allow a person forwarding an email to edit the message being forwarded. Such alteration would not be discernible to the recipient as such create a big risk as regards email authenticity.
In addition to the risk of email authenticity, every separate email forming part of a chain, may have been written by different authors along the chain, which creates the risk for hearsay. It is therefore not enough to simply print out the last email in the chain and attach the email thread to it as evidence of the email authenticity. It is advisable for the Lawyers to lay the foundation for the admissibility and authenticity of each separate email before seeking to tender such an email chain or thread as evidence.

Email certification and delivery

One of the technological avenues for ensuring the authenticity of emails is the use of the email certification programs.
An email certificate is a digital file that is installed to your email application to enable secure email communication. Not only does this authenticate the identity of the sender to the recipient, but it also protects the integrity of the email data before it is transmitted across the internet.
Luckily in Uganda, the Electronic Signatures Act, provides for a mechanism for the adoption and used of such certification services. Through the use of electronic signatures, it is possible to reliably identify the signatory.
Anyone intending to use this type of e-signature must subscribe to platforms of Certification Service Providers in order to be issued with certificates showing authenticity of the subscriber's e-signature. Both the signatory and the person relying on the signature must be in possession of a certificate.

In addition to email certification, one can also embed registered mail within their existing mailing systems. This is essentially the electronic (email) equivalent of postal "registered mail", providing senders with a register enabling the location (delivery status and reading disposition) of their emails to be tracked. This eliminates any claims of non-received emails.

Augustine Idoot
Partner

Litigation, Arbitration, Telecommunications, Media & Technology (TMT), Intellectual Property, Employment

KAA.CO.UG