ARTICLE:

Admission of Electronic Evidence: Contradictions in the Kenyan Evidence Act

By **Isaac Rutenberg, Stephen Kiptinness and Abdulmalik Sugow**

Introduction

Evidence generally refers to that which is used to prove facts in issue or facts from which facts in issue may be deduced (section 3, Evidence Act, 1963). The tendering of evidence in legal proceedings to prove or disprove assertions has been the practice for a considerable amount of time (Langbein, 1996) and as a result, evidence law has developed significantly in a number of legal systems. While evidence may be categorized in various ways,[1] this paper focuses on electronic evidence. In the development of evidence law – the procedures and rules governing the presentation of evidence in legal proceedings – analogue forms of evidence have historically been the main form contemplated, and used. The rules relating to the admission of analogue evidence, traditionally consisting of items such as articles of clothing or written statements, developed in a relatively straightforward manner, raising relatively minimal dispute (Schafer and Mason, 2017). However, the development of technology – leading to the production and use of electronic evidence (e-evidence) – has posed various difficulties for evidence law (Schafer and Mason, 2017). This is in part due to the challenging nature of defining – in certain terms – what e-evidence is. A clear-cut definition is often overly broad or overly narrow, and runs the risk of being rendered redundant by subsequent development in technology – a common occurrence. Schafer and Mason (2017) proposed the following definition, which is used in this paper:

> 'Electronic evidence: data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.' (p.19)

The above definition is not the only attempt at theorizing what does and does not constitute e-evidence; developments in technology have prompted jurists' attention to digital evidence and the rules relating to it (Karia, Anand and Dhawan, 2015). This definition also largely ignores the way in which the data is created, which is a particularly important factor in the reliability of the evidence. Nevertheless, the purpose served by attempting to delineate the scope of e-evidence – both for civil and criminal proceedings – is to determine the rules that apply. Questions abound regarding the admissibility, authentication, or even relevance of e-evidence. In response to the increasing use of e-evidence in legal proceedings, various jurisdictions have responded in two primary ways: attempting to analogously apply existing evidence law to e-evidence, or reforming evidence law to address e-evidence specifically (Schafer and Mason, 2017). These two approaches may also exist contemporaneously, supplementing each other.

Due to its nature, e-evidence may be highly volatile, prone to manipulation, or at risk of damage (INTERPOL, 2019). These characteristics justify the development of legal responses that are currently taking place around the world, including in Kenya. The challenges that arise out of these characteristics often relate to the authenticity and ultimately the probative value of e-evidence, and suggest that a different approach to admissibility may be preferable (Karia, Anand and Dhawan, 2015). Material used to prove or disprove facts in legal proceedings ought to be 'trustworthy' i.e., reliable and authentic (Mason and Stanfield, 2017). Whereas reliability refers to its ability to attest to the facts in issue, authenticity connotes the veracity of the evidence as relates to its origin;

[1] Direct or indirect; primary or secondary; digital or analogue.

that it is what it purports to be (Mason and Stanfield, 2017). For these reasons, it is often relatively easier to authenticate analogue evidence. The authenticity or reliability of e-evidence may be in issue on the basis of various components, amongst other things, the medium of storage, content, or form of the evidence (Mason and Stanfield, 2017). In identifying any of these components, a litigant seeking to render a particular piece of evidence inadmissible may allege alteration, a lack of reliability, or raise a question as to the provenance (Mason and Stanfield, 2017).

To address these challenges, evidence law has evolved, resulting in the introduction of various rules relating to the admissibility of e-evidence. These rules often stipulate conditions tied to the integrity of the computer system in question, the persons involved in the actions of retrieving the evidence, or the methods of authenticating the evidence. One such example is the Kenyan Evidence Act (1963). The Kenyan statute, in section 106B, categorizes e-evidence as documentary evidence and deems it admissible in certain conditions:

> 106A. Section 106B to apply in proof of electronic records
>
> The contents of electronic records may be proved in accordance with the provisions of section 106B.
>
> 106B. Admissibility of electronic records
>
> (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on paper, stored, recorded or copied on optical or electro-magnetic media produced by a computer (herein referred to as '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 where direct evidence would be admissible.
>
> (2) The conditions mentioned in subsection (1), in respect of a computer output, are the following –
>
> (a) the computer output containing the information was produced by the computer during the period over which the computer was used to store or process information for any activities regularly carried out over that period by a person having lawful control over the use of the computer;
>
> (b) during the said 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 the said activities;
>
> (c) throughout the material part of the said 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 content; 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 the said activities.
>
> […]
>
> (4) In any proceedings where it is desired to give a 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;
>
> (c) dealing with any matters to which conditions mentioned in subsection (2) relate; and
>
> (d) purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate),
>
> shall be evidence of any matter stated in the certificate and for the purpose of this subsection it shall be sufficient for a matter to be stated to be the best of the knowledge of the person stating it.

These conditions primarily relate to the computer system from which the evidence is derived. For example, whether the computer, in producing the

record, was performing its regular function. However, in order to successfully admit e-evidence in accordance with this provision, the section refers to a certificate, identifying the electronic record and giving particulars of the device involved, signed by the person responsible for the operation of the device in question. The section has been interpreted as requiring the certificate as a necessary condition of admissibility by an increasing number of judges in several cases as is discussed below.

Section 106B was added to the Evidence Act as an amendment in 2009 (Kenya Communications (Amendment) Act, 2009). Subsequently, in 2014, the Evidence Act was further amended to include section 78A (by the Security Laws (Amendment) Act, 2014), which provides simply that e-evidence shall be admissible:

> 78A. Admissibility of electronic and digital evidence
>
> (1) In any legal proceedings, electronic messages and digital material shall be admissible as evidence.
>
> (2) The court shall not deny admissibility of evidence under subsection (1) only on the ground that it is not in its original form.
>
> (3) In estimating the weight, if any, to be attached to electronic and digital evidence, under subsection (1), regard shall be had to –
>
> (a) the reliability of the manner in which the electronic and digital evidence was generated, stored or communicated;
>
> (b) the reliability of the manner in which the integrity of the electronic and digital evidence was maintained;
>
> (c) the manner in which the originator of the electronic and digital evidence was identified; and
>
> (d) any other relevant factor.
>
> (4) Electronic and digital evidence generated by a person in the ordinary course of business, or a copy or printout of or an extract from the electronic and digital evidence certified to be correct by a person in the service of such a person, is on its mere production, 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, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Rather than setting out conditions preceding admissibility, the section lays out considerations to be made in estimating the probative value of such evidence. These considerations include the reliability of the storage, generation or communication, the reliability of the maintenance of the integrity of the evidence, and the manner in which the originator of the evidence was identified. Unlike section 106B, section 78A makes no mention of the requirement to adduce a certificate as to, amongst other things, the provenance of the e-evidence, the integrity of the system, or its functionality. The effect of section 78A is to allow e-evidence into any legal proceeding, and to rely on the judge to determine the weight of the evidence based on relevant factors.

In light of the fact that section 78A did not repeal section 106B, the position relating to admissibility of e-evidence in Kenya has been addressed in the courts. Prior to the enactment of section 78A, the High Court dispensed with the certificate requirement, citing its absence as a mere procedural technicality not warranting an ouster of the evidence. According to the court, the evidence ought to have been admitted, and it is for the court to assess its probative value (*Mable Muruli v Wycliffe Oparanya & 3 others*, [2013] eKLR). A subsequent decision at the Court of Appeal found that, despite the introduction of the blanket declaration of admissibility under the provisions of section 78A, the requirement of a certificate as described in section 106B is a mandatory one which cannot be obviated by constitutional prohibitions against undue regard to procedural technicalities (*County Assembly of Kisumu & 2 others v Kisumu County Assembly Service Board & 6 others* [2015] eKLR). The Court of Appeal treated the certificate as a mandatory precondition despite there being no clear wording indicating the same within the Act. In other courts, judges have even gone as far as to state that the law 'requires' section 78A and 106B be construed conjunctively (*Idris Abdi Abdullahi v Ahmed Bashane & 2 others*, [2018] eKLR), a position not supported by the text of the Act or maxims of legal interpretation, as discussed below.

This uncertainty notwithstanding, the provision requiring a certificate as to the reliability of the

computer system is a dated one. Having its roots in English Law, which Kenya adopted following independence, it has long since been abandoned by English law in favour of a presumption of reliability (Quinn, 2001). Reasons for its abandonment include the onerous burden it places upon litigants, particularly where the opposing litigant may be in a better position to adduce such a certificate (Quinn, 2001). The presumption was supported by the Law Commission, and was based on Colin Tapper's assessment of computer unreliability: that errors are either immediately clear or result from input error, although Ladkin and others noted, in this respect:

> 'Reading the original paper, it seems to us as if Professor Tapper was not categorising "most computer error" further unqualified, but rather particular phenomena which manifest in the use of one specific sort of IT system, namely systems commonly used for clerical work (maybe, more specifically, for legal-clerical work). The Tapper Condition does not appear to us to hold in general.' (Ladkin and others, 2020, p. 3)

That assessment has since been found to be inaccurate, and thus the presumption ill-informed (Ladkin and others, 2020; Marshall, 2020). For the reasons argued herein, while the presumption of reliability is misguided, to consider admissibility without requiring a certificate, as provided by section 78A, is the proper approach. It is thus problematic that Kenya's Evidence Act maintains a provision interpreted as requiring a certificate, and does so in contradiction with another provision obviating the need for a certificate.

This paper contends that Kenya ought to reform the provisions relating to e-evidence in its Act in a bid to remove any contradictions, and avoid cumbersome hinderances to the admissibility of e-evidence. In doing so, it proposes that section 78A ought to take precedence and a presumption of admissibility ought to replace the current default of requiring a certificate prior to admission i.e., section 106B ought to be repealed.

Development of e-evidence in Kenya

Prior to independence, the Indian Evidence Act applied in Kenya (section 183, Evidence Act, 1963). In keeping with the principle of free proof, the law recognized the three forms of evidence, real, oral, and documentary (section 3, Indian Evidence Act, 1872).

Of significance to e-evidence is documentary evidence. Documents referred to matter inscribed on any substance (section 3, Indian Evidence Act, 1872), although the Act recognized photographed words as documents (section 3, Indian Evidence Act, 1872). In 1963, at the time of Independence, Kenya enacted the Evidence Act, 1963 ('the Act'). At the point of enactment, it was clear that the Act also primarily addressed analogue forms of documentary evidence. Nonetheless, the applicability of these provisions appeared to be extended to digital formats of evidence in certain cases. For example, in 1983, evidence in the form of tapes and audio cassettes were admissible pending verification of the functioning of the recorder in question (*Nobert Oluoch Obanda v Republic*, Criminal Appeal 62 of 1983 [eKLR]).

The principle of free proof – which applied in Kenya via the Act – obviates hindrances to proving facts while at the same time avoids negative inferences from the use of one form of evidence over another (Lin, 1993). However, in order for it to be effective, certain caveats were put in place. One such caveat is the requirement of authentication of that which is adduced in proceedings as evidence. That analogue forms of documentary evidence were primarily contemplated by evidence laws at the time of their enactment is important owing to the accompanying rules of authentication. Authentication of documentary evidence refers to ascertaining information as to authorship or an adducer's personal connection to the document in question. Essentially, a court must be satisfied that the document is what it purports to be in order for it to be admitted. This was, of course, in light of the possibility of forgeries or altered documents. This rule regarding authentication has been construed as a facet of relevancy, without which it would not be apt to admit the evidence in question. In pursuit of this authentication, courts developed the 'best evidence' rule which, according to some, may negate or limit the principle of free proof if misunderstood. The best evidence rule essentially requires that where possible, the best form of evidence ought to be adduced, and in relation to documentary evidence, this ought to be the original. The means of authentication that existed varied in relation to public documents, but generally included accompanying witness testimony as to the credence of the document, witness opinions on handwritings, expert comparison, or expert examination of distinctive characteristics of the document.

The advent of computers and the use of information technology in day-to-day life has increased significantly in the past twenty years, thereby leading to the increased use of e-evidence in proceedings. As stated previously, the two main responses in evidence law to these developments were either an extension of existing rules to apply to e-evidence or an amendment of existing laws to incorporate provisions relating to e-evidence. In Kenya, the first response to the development of computer technology was an amendment to section 65 of the Act relating to primary documentary evidence via the Finance Act (section 65, Finance Act, 2000). The amendment expanded the scope of documentary evidence to include microfilms, facsimile copies and computer print outs (section 65(5), Finance Act, 2000) i.e., these were to be subjected to the same treatment as documentary evidence. In dealing with the question of authentication of computer printouts, the amendment introduced the allowance of the use of a certificate attested to by a responsible person – the first mention of the certificate provision in Kenyan evidence law (section 65(8), Finance Act, 2000).[2]

Less than a decade later, the Act was once again amended to insert a number of provisions relating to e-evidence (Kenya Communications (Amendment) Act, 2009). While most of the amendments in the Amendment Act were made to give effect to e-commerce and online business transactions (section 36, Kenya Communications (Amendment) Act), the insertion of sections 106A and 106B contributed significantly to the provisions of rules regarding e-evidence. Section 106A prescribed that section 106B would apply in relation to electronic evidence, while section 106B essentially reiterated the provisions of the earlier amendments to section 65 that extended the rules of documentary evidence to computer outputs and mentioned the use of a certificate as an authenticating measure (Evidence Act, 1963).[3] Shortly after these amendments, the Act was once again amended, inserting section 78A, which marked a shift from the existing position on e-evidence (section 31, Security Laws (Amendment) Act, 2014). In accordance with the new provision, e-evidence is generally admissible, without any requirements as to certification (section 78A, Evidence Act, 1963).

The process of amending the Act as described above reflected the legislator's intent to keep abreast with developments in technology (National Assembly Hansard, 11 December, 2014, Afternoon Sitting, p.18 and 36). Indeed, analogously applying the existing rules of evidence to e-evidence is not necessarily simple, thereby necessitating novel approaches. In order to understand the difficulties faced by legislators in developing rules relating to e-evidence, it is necessary to discuss the unique challenges that technology poses.

Unique challenges for e-evidence

The law and practice of evidence have been greatly affected by the digital revolution. The various influences and issues generally fall into two categories: new forms of evidence, and new challenges for evaluating evidence submitted to the courts. New forms of evidence arise from the many ways in which modern society relies upon and interacts with electronic devices, sometimes without our knowledge or understanding. Although it is obvious that the digital revolution has resulted in new forms of evidence, the actual forms, sources, and volume of evidence are not always obvious, and many courts or parties to a court case may be surprised by them. The variety of new forms of evidence from electronic sources has been reviewed elsewhere (Weir and Mason, 2017), and is merely mentioned here.

With each new form of evidence, potentially new issues arise in terms of admissibility, authentication, and weight. Many digital records and data have (practically) no analogous form of non-digital evidence. Cellular telephone GPS records, keystroke logs, printer memories, and document version histories are a few examples of new forms of evidence that raise issues for which traditional jurisprudence in evidence is unlikely to be helpful.

Stanfield identifies a number of unique challenges of authenticating electronic evidence in litigation (Stanfield, 2016). These challenges result from characteristics of the evidence that are largely

[2] The literal wording of section 106 does not state that a certificate is a necessary precondition for admissibility of the evidence, but merely states that a certificate 'shall be evidence of any matter stated in the certificate and… sufficient for a matter to be stated to be the best of the knowledge of the person stating it'.

[3] However, like section 65, the literal wording of section106B also does not precondition admissibility on the submission of a certificate.

unknown or not problematic in non-digital forms of evidence, and include: unprecedented volume; ease of duplicability; persistence of the data; the existence of metadata; and the changeability of the evidence. Other characteristics, and the resulting challenges, have been identified and reviewed (South Africa Law Reform Commission, 2010, pp. 8-15). The challenges further metamorphosize when distributed and networked technologies are involved, such as cloud computing and blockchain technologies.

Admissibility, authentication, and weight become incredibly complex issues for even the simplest forms of e-evidence. An email passes through numerous systems and processes between sender and receiver.[4] Most processes are normally entirely automated but can be modified or monitored by a human with sufficient access, skill, and motivation. Once the complexity of the evidence is recognized, the inescapable conclusion as stated by Duranti, Rogers and Sheppard, is:

> 'The nature of electronic records challenges traditional rules of evidence and procedure, and requires their reformulation. For example, the traditional best evidence rule is no longer relevant because of the absence of an original in the digital environment. The authentication rule also is inadequate, because it cannot be established that an electronic record is the same as its first instantiation simply by looking at the record itself, but it is necessary to refer to an unbroken line of traces left by all those who interacted with the record or to the legitimate custody of a professional who can account for them. Furthermore, the complexity and variety of digital information systems and the often uncontrolled ways in which they are used, make it difficult to identify records within them and the business activities to which they are linked, thereby challenging the application of the business records exception to the hearsay rule. Finally, ever-changing technology speeds up the obsolescence not only of earlier record-making processes, but also of the laws regulating admissibility.' (2010, p. 98)

To an individual with little more than a basic knowledge of technology, understanding the complex manner in which a piece of digital evidence arrives in the court, as well as understanding the nature of the evidence itself, can be daunting tasks. Even if technological complexities are understood at a sufficiently deep level, they may merely raise an awareness of the ease with which digital evidence can be mishandled or forged. This is likely to cause the evidence to be distrusted, as the court itself does not engage in authenticating the evidence. The High Court of Kenya at Kisumu noted the uniqueness of e-evidence, particularly its ability to be manipulated easily in an undetectable manner (*William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 others* [2013] eKLR). Since, perhaps unlike its analogue counterpart, digital evidence will rarely be trustworthy on its face,[5] courts are required to turn to the testimony of experts with respect to the type of evidence generally, the specific evidence sought to be introduced, and the path by which the evidence reaches the court. This is best exemplified in *Republic v Barisa Wayu Mataguda* [2011] eKLR where the impugned e-evidence was CCTV footage of the defendant and the court noted with concern that by copying the footage onto a CD, the police had made it difficult for the court to ascertain whether the evidence had been tampered with. This was also the case in *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others* [2013] eKLR. This inherent fallibility of e-evidence, in particular of computer output, has been severally noted (Ladkin and others, 2020; Marshall, 2020; Ladkin 2020; Mason, 2017a).

A further challenge posed by e-evidence is its incompatibility with the best evidence and hearsay

[4] A single email must pass through a number of routers and servers, each potentially maintained by separate business entities, and potentially located thousands of kilometres apart. The email may be transmitted in encrypted or unencrypted form, and may be generated on any of a large number of proprietary and open-source platforms.

[5] Secured digital signatures and communications using public key certificates are types of e-evidence that are self-authenticating. Some evidence laws give preferential treatment to such evidence in terms of admissibility and weight. Nevertheless, even these forms of evidence have vulnerabilities, and are typically more technologically complex and therefore harder to understand by those without a technical background. For instance, see the discussion on 'non-repudiation' of digital signatures in 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).

rules. The best evidence rule requires submission of the best form of evidence, usually the original. The hearsay rule, on the other hand, precludes the admission of testimony by a person who did not perceive directly that which he or she is attesting to. These two rules, applied to e-evidence, reveal two primary difficulties: electronic records do not necessarily have 'originals' in a meaningful sense being invariably, in the visually represented form, copies or even copies of the initial data input, and they generally serve as recordings of what has been said by others i.e., hearsay. The application of these two rules is exemplified in two cases. In the first, *R v Stojananovic Milan alias Allan & Anor* [2008] eKLR, the court made a ruling on the admissibility of a recording and in doing so, stated that the burden of proving or establishing that a document is an original document is a criminal burden of proof beyond reasonable doubt, though this may be due to the fact that this was a criminal case. It held that the prosecution had failed to prove the originality of the tape it sought to adduce. In the second, *Mohamed Loge Hussein & another v Republic* [2016] eKLR, the court refused to admit printouts of M-Pesa (mobile money) transactions due to, amongst other things, the fact that the evidence amounted to hearsay, because the persons who obtained it (officers of the Criminal Investigation Department (CID)) were not present to testify. While it is correct to conclude that digital data has the potential to violate the hearsay rule, it is crucial to distinguish between the types of digital data one is dealing with. In this case, M-Pesa printouts are automatically generated from the service provider, involving no human intervention, and could therefore have been treated as real evidence (Mason, 2017b). Suffice it to say that it will have been helpful to have the officers responsible for seizing the information, or a suitable qualified employee from the service provider who procures the information, present in court to provide corroboration (by way of affidavit or otherwise) as to the authenticity of the M-Pesa statements.

In view of the challenges, and now-ubiquitous nature of electronic evidence, section 106B of the Act was developed to provide a framework for submission and treatment of e-evidence. The provision has been interpreted as requiring, as a prerequisite for admissibility, a certificate accompanying any submission of e-evidence. However, section 78A permits the submission of e-evidence without any such requirement. Addressing this contradictory response to e-evidence is crucial for the following reason: whereas e-evidence, as a rule of thumb, can be unreliable (Mason, 2017a), there are varying degrees and causes of that unreliability. For example, as noted by Ladkin and others, some computer evidence would satisfy what they termed the 'Tapper Condition' i.e., having immediately discernible flaws/faults due to their simplistic nature (2020). A lot of these are Operational Technology systems, which are hardware and software that monitor or regulate physical processes (Conklin, 2016) such as speedometers, and unlike Information Technology systems, ascertaining their reliability is relatively easier (Ladkin, and others, 2020). In view of this reality, it is problematic to treat all forms of e-evidence identically with respect to preconditions for admissibility.

Current Kenyan legal requirements for introduction of e-evidence

The challenges described above initially served to justify the onerous approach to admissibility and weighting of e-evidence as technology developed. In Kenya, the first notable and substantive change to the law on e-evidence was the introduction of section 106B. It introduced the use of a certificate accompanying e-evidence as an authentication mechanism. However, section 78A, the result of a subsequent amendment, provides, generally, that e-evidence is admissible (without stipulating that a certificate is a requirement). Below we argue in favour of a presumption of admissibility which would expedite the administration of justice while allowing for the disparate nature of various forms of e-evidence.

Sections 106B and 78A: contradictory provisions

Section 106B of the Evidence Act reveals the legislature's awareness of the unique challenges of e-evidence, particularly that these challenges mainly lie in the authentication of e-evidence. For example, subsection (2) focuses on the reliability of the computer in question – often the source of inaccurate or faulty electronic records. The section generally seeks to address the challenges of authenticity by classifying electronic records as documents, obviating the best evidence and hearsay rules and putting in place mechanisms to ensure authenticity. In subsection (4), there is introduced the use of a certificate that 'shall be evidence of any matter stated in the certificate…'. Such a certificate may be

tendered by persons seeking to adduce electronic records as documentary evidence.

Section 106B is problematic for a number of reasons, as discussed below. A major issue identified is the lack of certainty as to whether the requirement of a certificate is mandatory. Section 106B(4) can be distilled into the following relevant statement: 'In any proceedings where it is desired to [submit e-evidence], a certificate… shall be *evidence of any matter stated in the certificate* and for the purpose of this subsection it shall be sufficient for a matter to be stated to be the best of the knowledge of the person stating it' [emphasis added]. This is hardly a clear directive that e-evidence is not admissible in the absence of a certificate. The wording of the provision, as chosen by Parliament, essentially provides that the courts may make use of a certificate as a mechanism to authenticate electronic records. It goes no further than that, and certainly does not state that certificates are prerequisites, as has been held in some judicial cases discussed below. Unfortunately, it is not possible to settle this matter and to derive legislative intent from the Parliamentary records on either of the amendments; the two provisions appear to have been transposed from other jurisdictions with little policy informing the decision.

Section 106B was the dominant provision relating to admission of e-evidence until an amendment in 2014 introducing section 78A. The amendment in question did not repeal section 106B despite it providing for admission of e-evidence in a manner (according to this article) contrary to the provisions of section 106B.

Section 78A, enacted subsequent to section 106B, provides, simply, that electronic records are admissible. Much like section 106B (2), it obviates the best evidence and hearsay rules by providing that e-evidence may not be disqualified on the basis of being a copy. Similarly, it also focuses on the potential but most likely source of inauthenticity, the computer, in subsection (3). However, as opposed to requiring proof as to, amongst other things, the working condition of the computer, it simply provides that such aspects ought to be considered in weighting e-evidence. This tempered approach to the reliability of computer systems marks a move to recognizing e-evidence as a common occurrence in everyday life, and, despite inherent faults, that it ought to be admitted but then subjected to any dispute as to its soundness.

Conflicting jurisprudence

The mandatory nature of section 106B was not clear before the enactment of section 78A. The wording of the provision does not expressly place a mandatory burden on litigants to produce a certificate. In *Mable Muruli v Wycliffe Oparanya & 3 others* [2013] eKLR, the High Court applied article 159 of the Constitution of Kenya (2010) to admit evidence contained in CDs, citing the absence of a certificate as a mere technicality that ought not get in the way of justice. Article 159 urges courts to dispense with undue regard for procedural technicalities. The judge in the matter cautioned against equating admission of evidence with the court's being convinced by the evidence. The court found that the evidence ought to be admitted in its totality, and the probative value decided after the fact. It is instructive that this position is essentially replicated in section 78A, which was enacted a year after this decision.

Despite the enactment of section 78A, a number of cases have interpreted the certificate as a mandatory requirement (*MNN v ENK* [2017] eKLR*; Jack & Jill Supermarket Ltd v Viktar Ngunjiri* [2016] eKLR; *Dry Associates Co. Ltd & 3 others v Timothy Karungu Karanja & 7 others* [2019] eKLR; *Margaret Kariuki v Caroline Mutoko & 2 others* [2019] eKLR; *London Distillers (K) Ltd. v Mavoko Water and Sewerage Company & 2 others* [2019] eKLR).

The common approach adopted by decisions upholding the mandatory nature of the certificate is to argue that sections 106B and 78A ought to be contemporaneously applied. This was the case in *R v Mark Lloyd Stevenson* [2016] eKLR, *Republic v Betting Control & Licensing Board & 3 others ex-parte Diana Muthoni t/a DND Gaming Machines* [2019] eKLR, and *Idris Abdi Abdullahi v Ahmed Bashane & 2 others* [2018] eKLR, all before the High Court. In rationalizing a finding that the requirement is mandatory, the High Court held that, despite section 106B being the earlier of the two provisions, it gives effect to section 78A, in that it sets out the conditions in which the latter should be implemented, and that article 159 considerations are insufficient to displace this requirement of a certificate. (*Idris Abdi Abdullahi v Ahmed Bashane & 2 others* [2018] eKLR). Perhaps the most notable of these decisions that affirmed this interpretation of the Act, is the case of *County Assembly of Kisumu & 2 others v Kisumu County Assembly Service Board & 6 others* [2015] eKLR before the Court of Appeal.

In the cases described above, the Court of Appeal and the High Court reconciled the two provisions by interpreting section 106B as providing the only mechanism of certifying e-evidence. However, as noted above, section 106B simply provides that a certificate may serve as evidence. This significantly differs from perceiving the section as stipulating that the certificate is the one, and only one, means of certifying e-evidence. Further, the suggestion that section 106B serves as a mandatory operationalization of section 78A is a stretch, seeing as the latter was enacted after the former. In particular, the High Court in *Idris Abdi* went as far as to state that the law 'requires' this approach. This position is unsupported by the explicit wording of the Act, and contradicts all principles of legal interpretation as outlined in the next part.

Remedies in principles of interpretation

In the discussion of the interpretation of these two provisions, enacted at different times, two principles are relevant. The first is that the more recent legislation takes precedence over the former where a conflict exists (*Kenya Country Bus Owners Association & 8 others v Cabinet Secretary for Transport and Infrastructure & 5 others*[2014] eKLR). This typically applies where two provisions are diametrically opposed – the later provision would impliedly repeal the earlier, inconsistent one (*Kenya Association of Stock Brokers and Investment Banks v Attorney General & Another* [2015] eKLR). This is arguably the case in the Act, to the extent that the two provisions generally relate to e-evidence and reach opposite conclusions depending on whether or not a certificate is present.

The second is that a later general law does not repeal an earlier specific law (*R v Gwantshu* [1931] E.D.L.). On the face of it, and applied to the discussion at hand, section 106B, being the earlier specific provision, would survive even in the face of section 78A. However, section 106B is only 'specific' in that it provides a specific condition on the *general* admissibility of all e-evidence, and this principle may therefore not apply. Furthermore, there are exceptions to the principle. These exceptions require one to consider, amongst other things, whether the application of the earlier, specific law, would frustrate the purpose of the general law (Kaczorowska-Ireland, 2010). In *William Odhiambo Oduol v Independent Electoral & Boundaries Commission & 2 Others* [2013] eKLR, the onerous burden of certificates effectively precluded the petitioner from adducing evidence that may have resulted in a favourable outcome. One may argue that this frustrated the purpose of section 78A – to facilitate easy admission of authentic e-evidence. This reasoning is in consonance with the principle that the law should serve public interest (*Law Society of Kenya v Kenya Revenue Authority & Another* [2017] eKLR).

The 106B certificate: inherent flaws

If the discussion above that the Act, as is, does not make the adducing of a certificate mandatory is unconvincing, it is further contended that the provisions relating to a certificate ought to be removed in favour of a presumption of admissibility of e-evidence. This suggestion is grounded on the basis that section 106B, in detailing the use of a certificate, mandates an impractical and ineffective solution to a complex problem that often calls for ad hoc approaches, i.e., the certificate, as is, would fail to establish authenticity or reliability of e-evidence. These impracticalities and the resultant inefficacy are discussed below.

Ambiguities and shortcomings

A textual analysis of section 106B raises a number of concerns. Major ambiguities exist in subsections (2) and (4). To begin with, certain concepts and phrases remain undefined, and when applied to the dynamic nature of e-evidence, engender even further confusion. For example, the law makes mention of the phrase 'ordinary' or 'regular' activities in reference to the production of the computer output sought to be admitted as evidence. When it comes to ubiquitous general purpose computer devices such as smartphones, the challenge of this ambiguity becomes all too clear (see *Ndigwa Steve Mbogo v IEBC & 2 others* [2017] eKLR for an example of this impossible hurdle), i.e., just what is the regular activity of a smartphone? In addition to the device in question being subjected to this 'ordinary activity' standard, operators of such devices are also subject to the standard, yet the concept remains undefined. In *Ndigwa Steve Mbogo v IEBC & 2 others* ([2017] eKLR), the court rejected audiovisual evidence obtained from social media due to the fact that downloading videos from social media did not constitute the person's 'regular activities'.

In reference to the device, the section suggests that one ought to be able to attest to its 'proper functioning'. As has been alluded to earlier in this paper, computer software can be unreliable. Proving

reliability to the technical standard (i.e., system reliability) is often arduous. It is only possible to estimate a probability of error; this is unhelpful in legal contexts where such a failure may not appear immediately when software evidence in question is examined (Ladkin, and others, 2020). In addition to this, the concept of 'proper functioning', and a litigant's ability to attest to it, is based on two false beliefs: that computer reliability is binary; and that errors in e-evidence are immediately apparent to operators or owners (Marshall, and others, 2021).

Putting aside the fact that leaving this burden to regular lay litigants with little to no technical knowledge is unfair, 'proper functioning' is an undefined concept. If one were to assume that this 'proper functioning' is the technical standard discussed by Ladkin and others (2020), then the bulk of e-evidence would be not be admitted, whether actually reliable or not. If it were to adopt a more lax approach, it is unclear if reliability and authenticity would be guaranteed. Without a clear standard, a litigant merely needs to attest to the proper functioning of a computer (whatever that may be) and that would give the court a false sense of certainty that the e-evidence meets the threshold.

According to the section, the certificate also ought to attest to the fact that the record in question was produced under the lawful control of the person responsible for the device. While this would clear up any doubts as to the origin of the record, it does little to address the fact that evidence is malleable and could be tampered with along the chain of custody.

The wording opted for in the section is also exclusionary towards some forms of e-evidence. Section 106B generally deals with computer output such as printouts and audiovisual materials. Consequently, it focuses on the device that generates such output, requiring that the certificate detail the 'particulars' of this device. First, it is unclear what these particulars would be. Would litigants be required to adduce general details regarding the hardware, software, and ownership of the device? Would this vary depending on the device? Would such particulars necessarily or optionally include any system diagnostics or recent repair works done? Second, the use of the phrase 'device', and the focus on computer output generally ignores instances where the e-evidence in question is either an operating or application software (Weir and Mason, 2017). For example, in *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), the British Post Office's system, Horizon, was the e-evidence in issue. If litigants in that matter had to adduce a certificate that detailed the particulars of the device, any such information would be meaningless since the issue was a flaw in a software used by the Post Office. As it stands, even legal frameworks which recognise software evidence are insufficient. Marshall and others (2021), argued that the *Bates* decision highlighted an absence of clarity on the scope of materials which ought to have been disclosed in order to assess the reliability of software. In that case, relevant information such as Known Error Logs (KELs; a record of flaws discovered in the software) were not adduced without an order from the judge in this particular case. This highlights a major challenge in any evidence law framework – recognising the varied nature of different forms of e-evidence. In Kenya's case, such disclosure requirements appear not to be considered altogether, with litigants being required to merely attest to 'proper functioning' using a certificate. Adding to this difficulty is the fact that without clear disclosure requirements, litigants who find themselves having to challenge e-evidence are at a disadvantage due to the information asymmetry that persists.

To compound the above challenges, the certificate that ought to attest all this ought to be signed by a 'responsible person'. Where evidence may change hands numerously prior to arriving in court, it is not clear who this person is. This resulted in the disqualification of evidence in *R v Edward Kirui* [2010] eKLR, where the High Court found that the cameraman who recorded the occurrence of the facts in issue was not the appropriate 'responsible person'. Instead, an editor of the newsroom at the cameraman's employer was held to be the responsible person. With no prescriptions as to the technical qualifications of this responsible person, this requirement further compounds the hurdles facing litigants without guaranteeing courts of the soundness of the e-evidence. The requirement of a singular responsible person is also fanciful, considering that e-evidence may be the result of input from a multitude of different computers, all operated by different persons. Taking the example of bank ATMs, as explained by Mason (2017c), the range of witnesses required where the authenticity of e-evidence relating to ATMs is in question is considerably wide. It would be absurd if only one

person were to attest to all the prescriptions in section 106B(2).

The 106B certificate: impractical and ineffective

Aside from the concerns with the text of section 106B, other problems arise with the practice of using a certificate. First, requiring a certificate presents a barrier that may be significantly challenging or even insurmountable in the context of the Kenyan jurisdiction. An illustrative example is evidence from a user account on a social media platform. Given the wide availability of internet-connected mobile devices, evidence pertaining to criminal or tortious activity is increasingly obtained by ordinary individuals and uploaded to social media accounts, sometimes directly (i.e., bypassing the individual user device used to obtain the evidence). For example, video evidence relevant to a crime may be transmitted by a user device to Facebook Live, but the video may be stored on Facebook servers rather than locally to the user device. Requiring a certificate for such evidence raises numerous questions and significant challenges, since the people involved in the multi-step process of collecting, storing, and retrieving such evidence are numerous and often outside the jurisdiction of Kenya. This problem is compounded for 'viral' media that is transmitted between large numbers of social media users and, ultimately, may not be traceable to the originator of the data (Hasan, 2019). In such cases, the original device and the individual obtaining the original data are unavailable, but the data may still be accurate and relevant to legal proceedings. Requiring a certificate for admissibility effectively precludes this category of evidence, and may significantly hamper the submission of any evidence that is originally stored on platforms beyond the borders of Kenya. In *Ndigwa Steve Mbogo v IEBC & 2 others* [2017] eKLR, this hypothetical became reality when witnesses were barred from adducing video evidence downloaded from Facebook and YouTube due to the fact that, among other things, downloading social media videos did not constitute part of the responsible person's 'ordinary activities' as required by the Act. This implies that, in order for a litigant to adduce e-evidence obtained from social media, they would have to procure the services of an individual whose ordinary activities entails downloading media from these platforms.

Second, requiring a certificate is further problematic because it oversimplifies the issue, and may unjustifiably bias a judge toward finding a piece of evidence reliable, even where the certificate does not address reliability. As previously stated, the pathway for getting a piece of electronic evidence before a court, from original creation to final presentation, may involve a large number of electronic devices and modes of transmission. Alteration of the data, whether intentional or unintentional, can occur at any step in that pathway, including times that the data are in transit and at rest. Requiring a single certificate to guarantee admissibility of the evidence therefore ignores the continuity of evidence (also called chain of custody), a long-established principle in judicial systems. Aside from this, some of the conditions listed in section 106B (2), which a certificate ought to attest to, are practically difficult to satisfy, as has been discussed above. Furthermore, different types of e-evidence require differing levels of corroborating evidence in order to be credible. Measurement data, such as radar-measured vehicular speed, is not reliable without evidence of proper calibration and operation of the measuring device. In contrast, documentary evidence (e.g., emails) may simply require verification from the originator of the evidence (Ladkin and others, 2020). To apply a single, statutory method for gatekeeping all e-evidence ignores these nuances, and risks biasing a judge toward credibility where none is warranted.

Third, the preliminary threshold requiring certification of e-evidence from the beginning is not necessary considering that, where the e-evidence is admitted without certification, there remains an opportunity for the court to interrogate the evidence and make a determination as to its probative value and if any weight is to be attached thereto. The same mandate, of determining probative value, is provided for in section 78A which does not prescribe the use of a certificate. Since reliability and authenticity are always relevant issues, but the nature of such inquiries differs for different forms of evidence, the uniform requirement of a certificate for admissibility is inadvisable. In view of the suggestion to remove the requirement of a certificate, the discussion below discusses the modalities of the presumption of admissibility.

Presumption of admissibility

In the preceding discussion, this paper recognized the increase in the use of e-evidence, discussed the provisions relating to the admissibility of such evidence in Kenya, highlighted an inconsistency in the law and jurisprudence, and has argued against the

current default position of treating a certificate as a mandatory condition. In advancing this argument, this paper has identified an absence of clarity as to whether the certificate is mandatory, an inability of the certificate as envisaged in statute to guarantee reliability, and an unnecessary imposition placed on litigants by requiring a certificate when tendering e-evidence. However, this paper also notes that e-evidence can be unreliable, and therefore simply ignoring these faults is inadvisable. In this section, the paper proposes the adoption of a presumption of admissibility – that judges ought to admit e-evidence barring any legitimate concerns as to the legality of the process used to obtain it. This proposal is made by first asserting that there is a clear absence of policy behind the adoption of the use of a certificate in Kenya. While India's Evidence Act has the same provision (mandating a certificate), it does not have an equivalent to section 78A, which counters the certificate requirement.

As mentioned above, Kenya made use of the Indian Evidence Act prior to the passage of the Kenyan Evidence Act. The Kenyan Act came into force in 1963, and bore striking resemblance to the Indian Evidence Act, which it replaced. The introduction of sections 106B and 78A respectively took place in 2009 and 2014 – long after the Indian Evidence Act introduced its provision on admissibility of electronic records, section 65B (Indian Evidence Act, 1872) through the Information and Communication Technology Act (2000). The wording of section 106B is the same as section 65B of the Indian Act. This is attributable to a shared colonial history. In the parliamentary debate preceding the introduction of section 106B, no mention is made regarding the country's policy towards the reliability of e-evidence, or whether the provision is a suitable one (National Assembly Hansard, 13 November 2008, Afternoon Sitting).[6] Absent any clear policy indications as to why Kenya opted to include a certificate requirement (or provisions that have been interpreted as requiring a certificate), it is difficult to see why it should be maintained at the cost of section 78A's more open position.

Mirroring the High Court of Kenya in *Mable Muruli* [2013] eKLR, an Indian court found that the provision as to the certificate was not a mandatory one in light of pursuing the ends of justice (*Shafhi Mohammad v State of Himachal Pradesh*, SLP (Crl.) No. 2302 of 2017). This was contrary to a prior decision affirming the mandatory nature of the certificate (*Anvar P.V. v P.K. Basheer & Ors.*, (2014) 10 SCC 473) leading to general uncertainty in precedence. More recently, the Supreme Court of India laid to rest this conflict by affirming that the condition is a mandatory one (*Arjun Khotkar v Kailash Gorantyal*, (2020) 3 SCC 216). However, unlike Kenya, India does not have an equivalent to section 78A, which obviates the use of a certificate. Furthermore, this affirmation by the Supreme Court of India does not take away from the arguments made against the use of a certificate in this paper.

With the frequency and variety of use of technology in people's day to day lives, the admissibility of e-evidence ought not be a highly prescriptive process, or one that prevents the admission of evidence in instances where computer output is acquired with insufficient access to, and information regarding, the source (particularly where such evidence can be corroborated by eye-witnesses or by other means). At the same time, considering the various vulnerabilities of software, described previously, the certificate is not necessarily the only or best approach to e-evidence. Arguably, the provisions of section 78A, providing for general admissibility and prescribing a further assessment to be undertaken by judges in assessing probative value, is more appropriate. Provided that e-evidence has been legally obtained, and is relevant to the matter at hand, it ought to be admitted. Upon admission, judges can then conduct an examination as to the probative value of the evidence at hand, guided by the provisions of section 78A. In addition to the guidance offered by section 78A, courts may also determine the reliability of evidence using factors, such as the nature of the e-evidence, the likelihood of that evidence being altered by faults in a system (Ladkin and others, 2020), or the likelihood of intentional tampering or falsification. This position is not novel; it was adopted by the High Court in *Mable Muruli.* Possibly, in assessing this probative value,

[6] The link (https://info.mzalendo.com/hansard/sitting/national_assembly/2008-11-12-14-30-00) used to obtain access to this Hansard Record unfortunately is not paginated. However, it does indicate the name of the Bill being debated. The Official Parliament website does not have records dating back to 2008. The source website, Mzalendo, is an NGO that covers all matters to do with Parliament, to facilitate accountability.

judges would also be able to lean on either an expert or non-expert witness, depending on the particular facet of reliability in question, e.g., faulty human input or an inherently faulty computer. The type of witness would of course be dictated by the nature of the challenge posed by either party to the evidence in question (Mason, 2017c).

Other approaches such as the Commonwealth's Model Law on Electronic Evidence exist (Commonwealth Secretariat, 2017). In this Model Law, the Commonwealth suggests that system reliability, i.e., determining the probability of failure over a period of time, ought to be the standard used in assessing e-evidence. Further, it suggests a presumption of integrity of systems in certain conditions. These two provisions are not ideal. First, system reliability, as has been mentioned numerously in this paper, is not an attainable standard in every context. Second, adopting a presumption of integrity based on certain conditions such as the fact that an electronic record was developed by a party with adverse interests to the adducing party is misleading and distracts the court from critically assessing the e-evidence in question. The presumption of admissibility advanced herein makes no assumptions as to the soundness of the e-evidence, and leaves it to judges to determine on an ad hoc basis, with the help of witnesses, how much weight to assign a piece of e-evidence.

In determining this probative value, it is crucial for practice rules to be developed, detailing specific disclosure requirements in relation to different types of e-evidence. As suggested by Marshall and others (2021), requiring owners of software to disclose aspects such as Known Error Logs, service history, etc. can provide sufficient information for a judge to gain a clearer picture of the reliability of the evidence in question. This would perhaps overcome the challenges posed by a singular certificate which simplifies the matter of computer reliability, provides a false sense of security, and is wrought with ambiguities.

Conclusions

Electronic evidence is no longer novel in the legal system. As seen in the development of Kenya's evidence laws, early laws and regulations dealing with e-evidence were designed to account for the novelty and unreliability of early computer systems. Computer systems, however, have significantly increased in prevalence, and knowledge around their reliability (or lack thereof), is more common. While e-evidence can be unreliable, these inherent fallibilities are as diverse as the forms of e-evidence; judges are better equipped to assess the probative value of what litigants adduce, being able to call upon various witnesses to aid in this assessment. Since the Kenyan legal system does not feature juries, this burden of weighing the probative value of evidence rests with the judge. With the principle of free proof permitting the use of varied forms of evidence, and e-evidence varying in complexity and reliability, it is not appropriate to impose a single uniform burden for admissibility.

Sections 78A and 106B of the Evidence Act provide contradicting approaches to the admissibility of e-evidence. These contradictions have resulted in conflicting jurisprudence throughout the Kenyan judicial system. In the conflict, some decisions provide that certification is mandatory whereas others dispense with it, favouring admissibility. The latter approach is the preferred practice due to, among other reasons, the inability of certificates to guarantee reliability, and the encumbrance placed upon litigants. The interests of justice are better served in Kenya not by excluding e-evidence through antiquated requirements of certification, but by allowing a judge to have the discretion to assign weight to all evidence according to their assessment of the reliability of the process the evidence took to reach the court. This would not be a novel approach; it would simply be adhering to the provisions of section 78A.

Isaac Rutenberg holds a JD from Santa Clara University, a PhD from Caltech, and is the Director of the Centre for Intellectual Property and Information Technology Law (CIPIT), at Strathmore University in Nairobi. He is also a Senior Lecturer at Strathmore Law School and a practising patent attorney. irutenberg@strathmore.edu

Stephen Kiptinness holds a BSL and LLB from the ILS Law College, an LLM from the London School of Economics (LSE) and is a Senior Partner at Kiptinness & Odhiambo Associates. He is also a Lecturer at the University of Nairobi School of Law. stephen@koassociates.co.ke

Abdulmalik Sugow holds an LLB from Strathmore University, and was, at the time of writing, a Research Assistant at the Centre for Intellectual Property and Information Technology Law (CIPIT). He is currently interested in copyright law, platform liability, and political speech on social media. Further work: https://scholar.google.com/citations?user=A3tj_oQAAAAJ&hl=en

abdulmalik.sugow@strathmore.edu

References

Conklin, A. (2016). IT v OT Security: A Time to Consider a Change in CIA to Include Resilience. *49th Hawaii International Conference on System Sciences.* https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNzXFoB9/pdf

Hasan H. R. & Salah K. (2019) Combating Deepfake Videos Using Blockchain and Smart Contracts, in *IEEE Access*, vol. 7, pp. 41596-41606, doi:10.1109/ACCESS.2019.2905689

INTERPOL. (2019) Global Guidelines for Digital Forensic Laboratories

Kaczorowska-Ireland, A. (2010). *Public international law*. Routledge

Karia, T. Anand, A. & Dhawan, B. (2015) The Supreme Court of India re-defines admissibility of electronic evidence in India. *Digital Evidence and Electronic Signature Law Review,* 12. 33-37

Ladkin, P. (2020). Robustness of software. *Digital Evidence and Electronic Signature Law Review*, 17

Ladkin, P. Littlewood, B. Thimbleby, H. & Thomas, M. (2020). The Law Commission presumption concerning the dependability of computer evidence. *Digital Evidence and Electronic Signature Law Review*, 17

Langbein, JH. (1996). Historical foundations of the law of evidence: A view from the Ryder sources. *Columbia Law Review* 96, 1168-1202

Lin, TY. (1993). Making sense of documentary evidence. *Singapore Journal of Legal Studies,* 504 -537

Marshall, P. (2020). The harm that judges do – misunderstanding computer evidence: Mr Castleton's story 'an affront to the public conscience'. *Digital Evidence and Electronic Signature Law Review*, 17

Marshall, P., Christie, J., Ladkin, P., Littlewood, B., Mason, S., Newby, M., Rogers, J. Thimbleby, H., & Thomas, M. (2021). Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, 18

Mason, S. (2017a). The presumption that computers are 'reliable'. In Mason, S. & Seng, D. (Eds.), *Electronic Evidence.* (101-192). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

Mason, S. (2017b). Software code as the witness. In Mason, S. & Seng, D. (Eds.), *Electronic Evidence.* (88-100). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

Mason, S. (2017c). Competence of witnesses. In Mason, S. & Seng, D. (Eds.), *Electronic Evidence.* (339-349). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

Mason, S. & Stanfield, A. (2017). Authenticating electronic evidence. In Mason, S. & Seng, D. (Eds.), *Electronic Evidence.* (193-260). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

Quinn, K. (2001). Computer evidence in criminal proceedings: Farewell to the ill-fated s.69 of the Police and Criminal Evidence Act, 1984. *The International Journal of Evidence and Proof* 5, 174-187

Schafer, B. & Mason, S. (2017). The characteristics of electronic evidence. In Mason, S. & Seng, D. (Eds.), *Electronic evidence.* (18-35). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)

South Africa Law Reform Commission. (2010). *Electronic evidence in criminal and civil proceedings: Admissibility and related issues* https://www.justice.gov.za/salrc/ipapers/ip27_pr126_2010.pdf

Stanfield, A. (2016). The authentication of electronic evidence. (Unpublished doctoral thesis, Queensland University of Technology, Brisbane, Australia) https://eprints.qut.edu.au/93021/

Weir, G. & Mason, S. (2017). The sources of electronic evidence. In Mason, S. & Seng, D. (Eds.), *Electronic Evidence*. (1-17). (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)