Electronic evidence reforms: A comparative approach

THERE is an old aphorism that when you have a hammer everything looks like a nail. The unregulated use of electronic records in Nigerian courts appears to validate this adage. Increasingly, lawyers in a bid to showcase their mastery of technology are submitting evidence on a variety of digital formats. In some cases, copies of electronically stored information ("ESI") have been tendered as evidence without any clear protocol for their authentication or admissibility.

A case in point is the on-going trial of former Minister of Aviation, Chief Femi Fani-Kayode, on money-laundering charges. In a recent ruling at the Federal High Court in Lagos, Justice Ahmed Ramat Mohammed rejected a computer print-out of the defendant's statement of account as evidence. He opined that such a print-out was secondary evidence which was not authenticated and was, therefore, inadmissible under Sections 97(1)(h) and (2)(e) of the Evidence Act even if the print-out was relevant to the proceedings. Relying on UBA Plc v S. A. F. P. U (2004) 3 NWLR Part 861 p.516 at p.543 paragraph A-G, and the Supreme Court's decision in Yesufu v ACB Ltd (1976), ANLP Part 1, 328) the judge ruled that a computer printout cannot be admissible as an entry in a banker's book.

This ruling throws up a number of questions in relation to the handling of electronic evidence. When is an electronic record admissible as evidence? What level of expertise is required to authenticate an electronic record? Will an expert be required to certify the methodology used to forensically copy and establish the digital fingerprint of the record? In what circumstances will inter-modal production of electronic evidence be allowed? Given that ESI is a moving animal that is easily susceptible to accidental or malicious modification or destruction, will parties be penalised or pardoned for failure to provide key ESI in a regulatory or litigation context?

What recursive framework should be used for ESI search? What determinative factors should parties use to delimit the scope of relevant ESI in complex cases? What standard of care is to be expected of lawyers?

In an inter-connected world where electronic evidence is adnexa of litigation, our legal system must address these issues urgently. Failing to do so will create a purulent vacuum that poses significant downside risks to the fair administration of justice. For instance, we can now negotiate contracts by e-mail, modify them in a blog and breach them in an instant message ("IM"). How do you preserve IM and SMS text messages for long term judicial evaluation? Many courts now accept evidence on digital formats without a commensurate archiving capability to preserve such data. This patchwork of dvds, cds, usbs, and PDAs containing pdf, tiff, jpg, mpeg and MS files can easily be corrupted and rendered worthless.

In light of these developments, the National Assembly will soon commence hearings for the long awaited denouement of a thorny issue that has captivated the legal profession for the past few years - the reform of the Evidence Act to include the discovery and admissibility of ESI (e-discovery).

While new rules are needed to harmonise e-discovery, care must be taken not to import wholesale reforms, which are not suited to our legal system. E-discovery is

not amenable to a "one-size fits all approach" because it presents challenges which are unique to each jurisdiction. So, while it may be appropriate to adopt an international best practice model for collating, reviewing and producing relevant ESI, the procedure for the cooperative management of e-discovery must be tailored to the specific requiements of our jurisdiction.

A comparative review of e-discovery developments in the United States (U.S.) and in England and Wales (England) will highlight some of the variations adopted by these jurisdictions to suit their specific litigation dynamic. This allows us to assess the impact of each variant before deciding on the most suitable blend for our system.

The universe of discoverable ESI:

In both jurisdictions, an "electronic document" is broadly defined to include information readily accessible from any electronic device or media. All electronic documents are subject to discovery, disclosure and production. There are variations on the issue of "accessibility".

Pre-litigation and pre-discovery preservation of e-evidence:

The duty to preserve all ESI that might reasonably be required in a litigation or regulatory context is a common law obligation that commences once litigation is reasonably forseeable. The widespread adoption of technology means that ESI will constitute much, if not most, of the evidence used in future litigation and motion practice. The U.S. approach has been to provide a general baseline against which courts can evaluate preservation efforts on a case by case basis. In England, parties are required to discuss preservation before the first case management conference. The timing of ESI preservation in the pre-action phase is unclear.

Meet and confer mechanism

In the U.S., parties are required to meet to thrash out all key issues pertaining to e-discovery. Judges are also empowered to include provisions for e-discovery in a scheduling order. This reflects the understanding that early planning is essential to managing amorphous ESI-heavy cases. There is no such formal mechanism in England, but the parties are required to hold early discussions. As a result, many parties engage in an imperfect tango of minimal written communications, over-broad requests and unilateral action, which savvy courts now penalise.

Search and de-duplication methodologies:

ESI takes many forms and can be found on heterogeneous devices in many locations. This inherent adaptability creates a growing mountain of data that must be searched and sieved in an attempt to find relevant evidence. In U.S. v Safavian, 435 F. Supp.2d 36, 40 (D.D.C. 2006), the U.S. government obtained 467,747 e-mails from one individual, but sought to admit only 260. The problem of volume and duplication underscores the lack of consistency between parties in relation to the level of searches carried out.

Although keyword and Boolean searches are now defacto search standards, jurists now advocate the use of more precise tools such as fuzzy search, probabilistic search, clustering techniques and ontologies.

Privileged, confidential or protected material:

Privileged documents might include information that your adversary or competitors must not see under any circumstances. Some U.S. judges take the view that privilege has been waived once the affected documents are seen by the opposition on the basis that it is hard to un-ring a bell. In England, the opposition may use the document or its contents only with the permission of the court.

Form of production:

There is considerable conflict over the form the produced ESI must take. The U.S. rules permit the requester to specify the format in which the material will be provided, for example, native format or inter-modal formats. The rules in England require the parties to co-operate at an early stage as to the format in which ESI are to be provided. This ambiguity has created some difficulties with regard to post-production review. A further problem is the difficulty and delay involved in obtaining ESI from foreign jurisdictions, especially if data privacy restrictions apply.

Authentication:

A crucial part of the e-discovery process is the procedure for authenticating ESI at trial. Authentication enables the presenter of ESI to prove that it is what the presenter claims it to be. In the U.S., the document must be evaluated against the requirements of several rules. The courts accept that ESI raises unique issues concerning accuracy and authenticity which counsel must be able to address on the first try. In Vinhee v American Express Travel Related Services Company, Inc., 336 B.R. at 445, the defendant sought to recover $40,000 in charges from a California resident but was unable to prove the authenticity of electronic statements it presented at trial. The case was dismissed. In England, the onus is on parties to challenge the authenticity of a disclosed document.

Hearsay, best evidence and admissibility:

In the U.S., ESI offer for its substantive truth may qualify as hearsay if it is offered as a statement. This raises an array of questions and arguments related to hearsay exceptions and admissibility. E-mail has been ruled to constitute party admission. Photos, video images and concurrent observations recorded on mobile phones and PDAs qualify as present sense impressions, while contemporaneous commentary may be admitted as an excited utterance. These emerging issues pose a major challenge at trial. For instance, the best evidence rule requires an original copy of the evidence at issue in order to prove the content of a writing or recording. How do you admit a thumb-drive in Ife when the original ESI is on a server in Aba?

Penalties and sanctions for ESI destruction:

U.S. and English courts no longer accept that IT problems might be to blame for failure to keep or produce ESI, ruling instead that such failure is prima facie proof of

deception. In Zubulake v UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003), UBS repeatedly failed to comply with e-discovery obligations finally resulting in an adverse jury instruction and a jury award of $29 million in special and punitive damages. In Coleman (Parent) Holdings Inc. v Morgan Stanley and Co. Inc., 2005 WL 674885 (Fla. Cir. Ct. 2005), responsive electronic documents were discovered after the defendant's counsel had certified that all the relevant records had been produced. In light of persistent e-discovery violations, the judge instructed the jury to make an "adverse inference" that the defendant had attempted to conceal or withhold material evidence. The jury promptly awarded the plaintiff $1.45 billion.

Final thoughts

The exponential growth of ESI is a critical challenge for the Nigerian justice system. The ambiguity inherent in human language and the tendency for different generations and vertical communities to invent their own words adds to the complexity of finding relevant ESI. Any amendments to the Evidence Act to regulate e-discovery will require a careful balancing act between international best practices and the limitations of local expertise. In a society where the under-privileged have limited access to justice, we cannot afford to further alienate a majority of citizens from the benefits of the rule of law by imposing an onerous framework.

Finally, the impact of proposed reforms on a lawyer's duty of care must be weighed carefully by the Bar Association. The proposed reforms will impact on a lawyer's duty to provide competent representation, maintain client confidentiality and uphold the integrity of the profession. Since e-discovery is not taught in law schools, the amendments should be easily digestible. A useful starting point may be to benchmark the procedural and substantive reforms introduced by the Attorney General of Lagos State, Hon. Olasupo Shasore (SAN).

- John Okonkwo is dual qualified U.S. Attorney and UK Solicitor specialising in information governance and technology, with a focus on e-discovery and e-fraud. He is a Director of Governance & Cyber-crimes at Ducain Forbes and a consultant to Ilo & Okoli LLP. John is a regular writer on ICT issues for international legal journals, a contributor to e-Discovery conferences, and has served as an adviser to the Lagos State government on cyber-crime, privacy and data security regulatory matters.