Volume **6** (3) 2024 https://doi.org/10.5204/lthj.3692

Book Review

Stephen Mason and Daniel Seng (Editors) (2021) *Electronic Evidence and Electronic Signatures* (5th ed.) University of London Press

Rilwan F. Mahmoud
University of KwaZulu-Natal, South Africa

ISBN: 978-1-911507-26-0 ISSN: 978-1-911507-24-6

The propulsion of technological advancements over the last decade has highlighted several gaps in the laws of evidence in criminal and civil procedures worldwide. Re-enactments and amendments of rules of evidence in recent times across several jurisdictions have continued to incorporate novelties in admitting, authenticating, and assigning probative value to electronically generated information.[1] From questions such as, are AI-generated information documents? And, are AI systems in the banking industry discriminatory? Stephen Mason and Daniel Seng offer significant insights in their in-depth analyses and reimagination of the foundational doctrines of evidence, in light of these technological advancements in their fifth edition of *Electronic Evidence and Electronic Signatures*. The book, although published in 2021, continues to be a rich resource and repository for potential first principles of electronic evidence. Perhaps the most outstanding contribution of this edition is the authors' non-parochial approach to cross-examining evidentiary principles like the best evidence rule (Chapter Six), hearsay (Chapter Three), and presumptions regarding the immutable nature of electronic information and Artificial Intelligence (Chapter Five).

Regarding the 'Best Evidence rule', Mason and Seng reexamine the doctrine through the scope of digital information (p. 64, 247 & 440). While there are varied interpretations and evolutions of the 'Doctrines of the Best Evidence Rule', its essence has remained consistent. In admitting and authenticating a piece of evidence, the primary version is preferred, and the secondary version can be accepted under the appropriate circumstances. In the authors' words, "the common law 'best evidence rule' established that original material be used whenever possible … the party who claims to put the contents of a writing in evidence [to] produce [the original], or account for its absence" (p. 246). A central theme of the discourse is the critical examination of what constitutes the best evidence of all types of electronically generated evidence. The authors argue that, unlike documents that have original versions, statements that have first-hand accounts, and real evidence before a court, electronic evidence has a transient in and does not always fall in these categories of classification (p. 247). However, electronically generated data are still broadly considered under these traditional rules of evidence. Consequently, Chat GPT-generated texts, photorealistic images generated on Stable Diffusion and even printouts from automated teller machines can be authenticated as evidence using the same rules as a paper document.[2] To this end, the book offers practical alternatives that prioritize the unique nature

[1] Examples of this are the Evidence (Amendment) 2023 and the *Data Protection Act 2023* both in Nigeria, as well as the *Cybercrimes Act 2020, Electronic Communications and Transactions Act (ECTA) 2002* and the Law of Evidence Bill 2014 in South Africa. See also Rilwan. F. Mahmoud *An Analysis of the Judicial and Legislative Attitude to Hearsay Electronic Data in South Africa* (2023).

[2] Stable Diffusion is an advanced deep-learning model that translates textual descriptions into detailed images.

of generating, storing, and reproducing electronic data in all its forms. Chapter six, in considering the difference between paper or other analog media and electronically stored information, highlights six best practice guides in authenticating electronic documents including metadata, volume and duplicity, persistence, dynamism, environmental dependency, and dispersion (p. 240).

Chapter nine goes even further, advancing an all-applicable classification of evidence of primary and secondary versions that applies to electronically stored information. The chapter deviates from classifications like original, duplicates, and certified true copies which applies to authenticating documents instead, it uses 'first in time' in referring to the 'original' version of electronic information. The first-in-time classification recognizes that an identical paper copy of an electronic message does not necessarily carry all the relevant information to determine its authenticity such as date, time, delivery status, and other metadata. Accordingly, the book posits two essential prerequisites to authenticating and admitting secondary versions of electronic information. The first requirement is that reproducing electronic information to be admitted as evidence 'should not alter the first-in-time' version and the second is that the proposed true copy 'should produce an exact copy' that includes all necessary metadata (p. 441).

Another significant insight from this book is the discourse on the reliance and probative value of electronic information, which Mason and Seng address extensively (p. 283-285 & 451). Proving electronic information to be authentic is one thing, verifying and presuming its content to be true is a completely different affair. Chapters seven and eight on electronic signatures and data encryption provide some insights on this topic. While appending physical signatures, stamps, fingerprints, and verbal confirmation are often adequate in confirming the genuineness of evidence, their endorsements on digital messages may not enjoy the same reliability or serve as an affirmation of the truth of their content (p. 288-290). Consequently, in several jurisdictions, higher evidential hurdles of presumption and proof are placed on electronic information as a reactionary measure to rapid technological advancements and in some cases, requiring certificates attesting to the content of electronic records (p. 299-301). Mason and Seng examine the implication of electronic signatures like personal identity numbers (PIN) encryption keys, biometrics, and the like, on establishing presumptions and the burden of proof. Furthermore, the book discusses the potential of encryption in allaying the scepticism associated with relying on electronic messages. The book highlights various ways in which encryption can prove intent, confirm the identity of the sender, recipient, or signatory to an agreement, or certify that a record is a true copy of the first-in-time record. The book reveals a dire need for a unified standard of authenticating and admitting electronic information. While some jurisdictions have relaxed the high premiums placed on electronic evidence, there is an urgent need for a departure from the traditional rules of evidence in evaluating electronic information.[3]

The central theme of the chapters in Seng and Mason's book is the reimagination of the first principles of evidence through the lens of electronically generated and stored information. Each of the chapters challenges the category bias in evidential classification, with a view to highlighting the underlying nature of all forms of electronic information. A criticism of this book, if it can be called a criticism, is that it does not include a model practice direction for judges, lawyers, law enforcement agencies, and policymakers, for which the book was undoubtedly intended. A model practice direction that reflects the critical analysis the book provides will be an invaluable tool to legal practitioners and judges alike especially where there are lacunas in their laws.[4] Directions on what constitutes primary and secondary versions of social media posts and emails, definitions of the role of metadata in proving the content of electronic records to be true, or stipulations on presumptions and burden of proof of electronically generated information can be instrumental in creating policies and legislations worldwide. It is expected that a subsequent edition will include some guidelines.

Bibliography

Mahmoud, Rilwan. F. "An Analysis of the Judicial and Legislative Attitude to Hearsay Electronic Data in South Africa." *Digital Evidence and Electronic Signature Law Review* 20, no 1 (2023): 10-29. https://doi.org/10.14296/deeslr.v20i.5566.

[3] Certificate required to accompany electronic evidence by Section 84 of the *Nigerian Evidence Act 2011* has been interpreted to include a simple oral testimony. Also, the South African *Computer Evidence Act* which had a similar requirement has been repealed.

[4] Appendix 2 is a 2016 generic draft convention on electronic evidence by Stephen Mason imported from a previous edition, but it does not contain a detailed practice direction.