Singapore Journal of Legal Studies
[2008] 219–223

BOOK REVIEWS

Electronic Evidence: Disclosure, Discovery and Admissibility BY STEPHEN MASON, ed. [London: LexisNexis, Butterworths, 2007. lxxiv + 551 pp. General: £125]

Electronic evidence (both analogue and digital) is frequently admitted in courts daily these days, as we are by and large dependent on, or affected by electronics in almost everything we say or do. Paper sources, hitherto the mainstay of records and documents, are already receding in importance, and even when used, are often 'hard copies' of electronic documents. Yet, the mainstream texts on evidence so far have not really tackled the problems of electronic in any detail. True, electronic evidence is just another form of evidence—distinct from oral evidence, and often regarded as just another species of either documentary evidence or real evidence. However, its unique nature makes it more difficult to authenticate as compared to other forms of physical evidence, such as paper documents. Ironically, the age of the computer brought about simplification of the best evidence rule in paper documents; so much so that copies are now readily accepted (though not in all jurisdictions) because of the accuracy of digital copiers in reproducing paper originals. The receivability of electronic evidence, on the other hand, is another matter as it can be multi-source, multi-form and multi-format. The fragility of storage media, ease of alteration or corruption of stored data, complexity of computer systems all adds to the difficulty of establishing a sound evidential foundation. Paradoxically, there is also the view that courts may attach too much weight to electronic evidence once admitted, as they may be overwhelmed by the technology (as for instance computer generated reconstructions of incidents that may not, but claim to be, accurate as to what actually happened).

This book is most welcome in that it may go some way to help address the fears and concerns of admitting and using such evidence. Stephen Mason (and his team of specialist contributors) should be commended in providing a work of this scope, which contains both general commentary and reports from specific jurisdictions. It should be understandable even for those who are not familiar with the technology unlike some electronic evidence works (mostly from US authors) that are written more for cyber forensics investigators than for 'laymen'. While works on cyber forensics are perhaps not for the ordinary lawyer, there is no doubt that lawyers involved in cases that rely on electronic evidence would need to at least understand its nature and how to use it: after all, it is now widely accepted that "electronic ignorance is NOT bliss." This is palpably true in the case of electronic evidence and

this book is especially suited to inform and guide lawyers seeking to find their way through the electronic jungle.

The reader of the book is immediately made aware that the pre-requisite to understanding this type of evidence is a threshold knowledge of the technical aspects of digital devices like stand-alone computers (combining hardware, firmware and software to 'render' output, which can be stored digitally) and extending to how such computers operate in networks, using various communications protocols and finally, how they connect to the worldwide web. Partly to make the subject understandable to the reader unfamiliar with the jargon, a glossary may be found at the beginning of the book. Perhaps the addition of diagrams and illustrations, especially on such terms as networks and metadata would make the terms more understandable to such readers. Also, more terms such as 'macros' and 'storage formats' (there are references to NTFS, Solaris ZFS) may need to be included. The explanation on 'operating system' is too brief to be helpful, and even teleological as it is given in the glossary; the one on 'application software' even shorter (though it is difficult to imagine readers not knowing what that term means these days, provided they use computers).

Chapters 1–5 together with a rather unusually lengthy preface are general in nature, describing the technical aspects of electronic evidence, and providing a useful classification of such evidence (somewhat oddly, in the preface and not the main text) and the problems that one can face in dealing with such evidence, whichever the jurisdiction. In the preface, the objective of this book is stated to be "to offer judges, lawyers, legal scholars and students an insight into the complexities of electronic evidence in its widest sense" (Preface). Mason goes on to describe what would be two distinct parts of the book. Part 1 (Chapters 1–5) would be the general part. It comprises roughly half the text of the book. Part 2 consists of what could loosely be referred to as country reports and surveys of how electronic evidence is received (though many of them contain discussions of the substantive laws relating to computer crime).

Part 2 comprises eleven chapters from selected common-law jurisdictions, South Africa and Scotland. The choice of these jurisdictions, and the omission of others like Malaysia, is not explained. Of this part (around 388 pages), over a quarter is devoted to the chapter of the law in England and Wales. Although this gives a lopsided look to this part, it is probably justifiable by the tendency of lawyers in other countries to turn to the law in England and Wales for reference. But there is no doubt that Mason, who is responsible not only for the general part (other than Chapter 5, which is by Schofield and Goodwin), but also the chapter on England and Wales, is not just the general editor but also the major contributor to the work and for that, he is to be especially commended for the work he has put in, and the much more in-depth analysis of the relevant evidence rules and doctrines applicable to electronic evidence.

Mason's view that "considerably more attention may have to be paid to demonstrating the integrity of digital data in the future" (p. 39) is one shared by many. His Chapter 3 on the investigation and examination of digital evidence, together with Chapter 4 (on evidential foundations) deserve careful reading especially for those lawyers preparing for cases that involve handling electronic evidence. The enormity of the task, not to mention costs, in dealing with electronic evidence comes out clearly in Mason's discussion of the various aspects of going through such evidence

and laying the basis for obtaining, handling, authenticating and admitting the evidence. In complicated cases, digital forensic experts may have to be called to explain not just the contents (the actual relevant evidence) but also how it came to be, how the output was generated, and how the integrity of the fragile evidence was maintained assiduously to avoid tampering or corruption. To be sure, the technological developments especially in storage devices (RAID arrays for example are now very common) and the existence of back-up software and procedures for off-site back-ups would make losing data by accident a thing of the past. But there may still be a real problem of intentional alteration or erasure, which are, in many cases, extremely difficult to prove or even provide evidence to establish.

In his discussion of cases from several jurisdictions involving alleged unauthorised withdrawals from ATM machines, Mason shows the disparity in approach by judges in dealing with digital evidence of *prima facie* valid cash withdrawals. The banks relied on their computer generated records to rebut claims for the return of the money withdrawn, even though they often failed to lay a proper foundation as to why such records should be received in evidence and whether the evidence is credible enough to counter the owners' testimonies that they were not the ones withdrawing the money.

These cases reveal that there are very real dangers of courts attributing too much weight to electronic evidence, and not being made aware of the weakness not only in terms of the integrity of the hardware and software, or the authenticity of the data, but of the factual inferences that could be drawn from them. For example, the fact that the digital recordings of withdrawals from the ATM machines appear normal does not allow for a compelling inference that the owner of the ATM card must have been either fraudulent or negligent. There may be other equally plausible inferences, such as the likely cloning of ATM cards and surreptitious copying of PINs without the knowledge of the owners. Mason rightly criticises those decisions that place too much weight on the idea that electronic evidence trumps human testimony.

Equally if not more serious, the ATM cases also show that undue reliance on electronic evidence may have the effect of placing unreasonable burdens on defendants, as for instance, in civil or criminal actions for fraud and theft, allegedly committed by the owners of ATM cards. In criminal prosecutions a defendant might be found guilty if he did not at least provide evidence to show he was not the one using the card to withdraw the money (such as in *R v Cochrane*, referred to in text at p. 69, para 4.05), where the defendant was initially convicted of theft, but the conviction was quashed on appeal). Mason also alluded to the fact that to place a burden on the owner to prove that a fraud was perpetrated on the bank by person or persons unknown is to place an unjustifiably heavy burden, given that the owner may not know specifics about the ATM transactions, or have the wherewithal to hire lawyers and forensic specialists to 'discover' the same for the relatively small sums at stake. Indeed one might be tempted to argue that as the electronic processes of a bank are peculiarly within the knowledge of that bank, it should prove that there was no unauthorised withdrawal from its ATM machines, or if it is a criminal case against the ATM card bearer, the prosecution should have a similar burden. Mason (at p. 82, para 4.15) suggests an evidential burden on the bank "to show that it is impossible for the PIN to be obtained by any of the known attacks used by criminals, as indicated in the technical literature." The wider issue is whether placing such burdens (be they

legal or evidential) on the financial institutions would have the undesirable outcome of leading to more instances of fraud or carelessness on the part of customers. It is however a question for substantive banking law and policy, and not really one for the law of evidence.

One of the most useful and interesting discussions for practitioners contending with digital evidence is in Chapter 4 (para 4.16, p. 88 *et seq*) dealing with steps to be taken to 'authenticate' digital objects. Quite rightly the traditional distinction between 'original' and 'copy' used in documentary evidence so far is out of place in relation to digital output. Mason's reference to three terms 'used in relation to the authentication of digital data' (para 4.28)—'authentication' itself, 'integrity', and 'reliability', however, seems over-ingenious: these are not terms of art, and one is unsure how or what Mason wants to do with them. As described they do not seem mutually exclusive. One would have thought (perhaps too traditionally) that one authenticates digital evidence to be tendered by proving its *first* source(s), its integrity by proving the system wherein it resides and is taken from and its reliability (to be used as evidence) by proving no unauthorised changes to the stored data, or unauthorised intrusions to the system that might affect the proffered output or the part of the system that stored it. Once the electronic evidence is authenticated, its admissibility or exclusion in terms of the other rules of evidence (like hearsay, character, opinion) would still need to be tackled.

What is perhaps special about electronic evidence is that its authentication can be a very complicated matter, as digital output can differ according to the hardware used to display it, as much as the software. There may also be digital enhancements or editing or changes in metadata that need to be explained to prove the reliability (or integrity) of the output to be used as evidence. One could not agree more with Mason's observation that "where the authenticity of a digital object is in (sic) issue, the range of considerations to be taken into account will differ, according to the nature of the evidence to be authenticated and where the evidence is to be found" (para 4.35). It could perhaps be possible to leave it at that, with examples of how simple and complicated the process of authentication might be. Chapter 5 (Using Graphical Technology to present evidence) deals with another problem altogether—but it is an important one, and that is the use of computers to assist in the presentation of evidence. The authors (Dr Schofield and Lorna Goodwin) very capably analyse the issues of using graphical simulations or re-constructions of events in presenting 'facts' before the court, especially in jury trials. They cite studies suggesting that an average person retains visual information (65–87%) much better than oral information (10–15%) and this fact alone must raise serious questions for the regulation of the use of visual means to present evidence. The advantages and disadvantages of using such evidence are well discussed by the authors.

Before one moves on to consider briefly the chapters on specific jurisdictions, one must mention that it would be most helpful, at least in the more lengthy chapters, to have a synopsis or an outline of section headers in each of them so as to assist the readers in determining the scope of the coverage as well as to enable them to focus on the topics they want to delve on. This is also pertinent in the case of the chapter on England and Wales, as that is a very lengthy chapter, full of sub-heads. Also, there are errors in editing, the most glaring of which is that Chapter 5 is titled "IT in the courts" in the Table of Contents and "Using graphical technology to present

evidence" in the actual chapter. More careful editing and proof-reading might be required in the next edition.

As for the chapters on electronic evidence in various jurisdictions, they are all written by specialist contributors from them. The jurisdictions are: Australia, Canada, England and Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States. As Mason explains in the Preface (p. xii), an outline of topics was agreed, though it was not possible to implement that in every jurisdiction. One perhaps unintended result is that there is much repetition about the best evidence rule, definitions of hearsay and exceptions, all of which are usually dealt with in the traditional evidence texts of each jurisdiction. Unfortunately, in certain accounts such as the ones from Hong Kong and India, a wide-ranging discussion, not only of electronic evidence but also of substantive law relating to computer crime and sentencing is found. This surely was not necessary in a book on electronic evidence, except insofar as such laws have special provisions on evidence. (One hopes to be forgiven here, as a reviewer from Singapore, for mentioning that the Singapore chapter is a good example of focussing on the subject at hand.) But by and large, the 'country reports', for want of a better term, demonstrate the growing awareness of the importance of electronic evidence and of the problems besetting them though the rules may differ as to how much a party may need to do in order to admit such evidence, or to challenge it. An additional chapter to examine common issues faced in the various jurisdictions, and the relative merits or demerits of each country's approach to electronic evidence might be very useful.

Finally, it may be added that this being by and large a practitioner's text, even broader law and society questions about the need for, and justification of, legal powers to have increased powers of surveillance, search and seizure in collecting electronic evidence are not really discussed. Privacy issues, such as users being required to provide passwords or decryption keys to their encrypted data, require the attention of legislatures worldwide, especially in relation to the control of international crimes, such as money-laundering or terrorism. A last section, then, on what the future holds in terms of technology developments and legal developments might also be a useful addition to what is already an enormously useful text that should have a place in the shelves of every legal practitioner and law firm.

CHIN TET YUNG
National University of Singapore