Book Review

ELECTRONIC EVIDENCE: DISCLOSURE, DISCOVERY & ADMISSIBILITY, by Stephen Mason (General Editor), LexisNexis Butterworths, 2007, lxxiv and 551 pp including index. New Zealand price $359 (hardcover).

Increasingly much of what is tendered in courts as evidence depends to some extent on digital technology. This book is the result of a significant endeavour to provide insights for legal personnel and students into the complexities of electronic evidence. As the preface notes, lawyers and judges now routinely deal with digital evidence, often despite being unaware that they do so. Accordingly, the book advises that as electronic evidence pervades all areas of law, lawyers must ensure they are acquainted with its intricacies. Add to this the somewhat alarming way in which virtual world disputes are being litigated in real world courts, and it becomes increasingly difficult to argue that electronic evidence is a specialist area of legal practice.

The range of available electronic evidence is vast – the preface gives a number of examples ranging from the regularly relied upon email, to videos taken on mobile phones, to the use of spyware in an industrial espionage case. There are innumerable others, and New Zealand readers will immediately think of our own notorious examples. Mark Lundy's mobile phone helped to pinpoint his whereabouts at the time his wife and daughter were murdered, and one of the central facts at issue in the Bain trial was who left the infamous message on the family's computer.

The book is edited by Stephen Mason who also contributes the first four chapters on general matters such as sources and characteristics of digital evidence; investigation and examination of digital evidence; and laying the evidential foundations. The remaining chapters are written by specialist contributors, all of which bar one cover jurisdictional approaches to the issue of electronic evidence. The exception is Chapter Five, by Dr Damian Schofield and Lorna Goodwin, on graphical technology in the courts.

Chapter One provides a necessary explanation of the technical issues involved, greatly assisted by the comprehensive glossary that precedes it. While most of us may know how to use a computer, understanding how one works is an entirely different matter. Yet assessing and using the electronic evidence available in any given case requires at least a rudimentary knowledge of the sources of digital evidence. Thus, Chapter One canvasses the basic principles including those involved in information storage and retrieval; the different types of files found on a computer including system and program files, temporary and cache files and deleted files; and some of the particular problems that are created by, for example, malicious software and encryption techniques. In respect of the latter Mason provides an interesting example. While one ordinarily thinks of encryption as beneficial in terms of security of data when engaging in online banking, for instance, it is also used by persons engaging in criminal activity to hide their activities when using the internet and email. Obviously this poses problems for investigators, who need to ascertain the content of encrypted files. In a child pornography case, *United States of America v Hersh aka Mario* (United States Court of Appeals for the Eleventh Circuit No 00-14592 July 17, 2002 before Anderson and Marcus, Circuit Judges, and Middlebrooks, District Judge), a Zip disk containing encrypted files was found in Hersh's possession. On Hersh's computer, investigators found software used to encrypt the files on the Zip disk. Obtaining a partial source code from the

manufacturer, the investigators were able to interpret certain information about the files on the Zip disk, including file names containing words that were consistent with child pornography. The list of files was compared against a government database of child pornography, which revealed that 120 of the files on Hersh's disk matched names on the database, and 22 of those had the same number of computer bytes as the files on the database. Thus, even though decryption was not possible, investigators established a sufficient link between the files possessed by Hersh and evidence of child pornography already known to authorities.

Chapter One also notes that the computer clock figures large in digital evidence. Again the cases of Lundy and Bain provide New Zealand examples in which the times computers were turned on or off were relevant to establishing times of death. Mason illustrates by reference to the notorious English case of Harold Shipman, the doctor convicted for intentionally killing a large number of his patients. It was alleged that Shipman altered medical records after the killings to give the appearance that the patients had been ill for a time prior to death. An expert gave evidence that it was possible to alter information in the records and then change the date of the computer clock to hide the fact that the alterations had been made. As Harold Shipman discovered in the course of his prosecution, while it is possible to change the clock on the computer to hide the fact that records have been retrospectively altered, it is almost impossible to hide, at least from a forensic examiner, the fact that the clock itself had been changed.

Thus, as the book makes clear, computers can produce large quantities of evidence even where every attempt is made to delete or hide files. For instance, investigators can look for evidence of email traffic, long after emails have been deleted. Furthermore, a great deal of skill is required to remove all traces of activity, and such skill is rare.

In continuing to lay the foundations for an understanding of electronic evidence, Chapter Two discusses the characteristics of electronic evidence, noting firstly the distinction between analogue and digital forms of data. One of the significant characteristics of digital data is its metadata, or 'data about data' such as when a document was created, by whom (ostensibly), the file type, and when it was last modified. Metadata, in digital documents, is generally hidden from the text viewed on a screen but such information is crucial in interpreting the evidential value of the digital data.

Compared with other forms of forensic analysis, the investigation and examination techniques associated with digital evidence are still quite new. Chapter Three looks at the role that experts play in identifying, gathering, analyzing and preserving digital evidence. Mason notes that there is recognition within the field of the need to distinguish between the different roles an investigator may have in these areas. He refers to three broad categories of personnel engaged in digital evidence forensics – technicians who responsible for gathering data, examiners who process particular kinds of evidence, and investigators who have responsibility for the overall investigation – each of which requires distinct levels of training.

This thread is picked up again in the next chapter, with the point that in order to establish the reliability of digital data, it is necessary to ensure that the relevant witness is qualified. Chapter Four thus canvasses evidential issues and the challenges inherent in laying a foundation for such evidence, particularly where authenticity and reliability questions arise. Mason also clears up a common misunderstanding in noting that it is not always so that intricate details of a computer's operating system are required for electronic evidence to be admitted. He points to email as an example – the fact that email can be forged is not a ground for such evidence to be automatically excluded, as in that regard there is nothing distinguishing emails from paper documents in their susceptibility to alteration or forgery.

With a topic this technically complex, particularly in a book of this length, there is a risk of the text becoming tedious. Mason avoids this by infusing the subject with vivid examples, such as the ones referred to above. This allows the reader to engage more readily with the subject matter, and is a skill also demonstrated to varying degrees by other authors.

In the first of the chapters authored by specialist contributors, Dr Damian Schofield and Lorna Goodwin tackle the use of graphical technology to present evidence in Court, noting that the increase in the use of such technology is supported by research that suggests that jury members retain a greater proportion of visually presented information than information orally presented. The authors refer to a number of cases in which computer-generated animations, for instance crime scene reconstructions, were used to explain the issues to juries.

Chapters Six to Sixteen cover, in alphabetical order, the evidential issues arising and relevant law applicable in Australia, Canada, England and Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa, and USA. The wide-ranging coverage is one of the book's strengths, bearing in mind that while all jurisdictions covered have a common law basis, there is significant variance in approach to evidential issues. While Mason notes that the section on England and Wales is larger than the others due to the publisher's requirements, the remaining chapters do not suffer in terms of depth. There is a shift in style, but this is expected in a book to which a number of authors contribute, and it does not detract from the readability of the book.

New Zealand's approach to electronic evidence is covered in Chapter Twelve which is authored by Laura O'Gorman, a partner at Buddle Findlay. O'Gorman records the passing of the Evidence Act 2006, which has subsequently (on 1 August 2007) come into force. Interestingly, since the Act's commencement one of the Court of Appeal's first decisions under the Act, *R v Petricevich* [2007] NZCA 325, concerns the admissibility of evidence of text messages used to identify an alleged drug dealer.

O'Gorman points out that in New Zealand there are guidelines for electronic crime investigation which prevent police officers involved in conducting searches from examining any electronic equipment found. Instead any such equipment is to be removed and examined by forensic experts. This is due to the fact, as pointed out earlier in Chapter Four, reliability issues arise if the person giving evidence of the data gathered is not qualified to do so.

As O'Gorman points out, in New Zealand at least much of the wording in statutes is intended to be technology-neutral, so that it can be applied in an ambulatory way. The desirability of this approach is supported by the authors of Chapter Ten (India). Manisha T Karia and Tejas D Karia refer to the recognition by the Indian Supreme Court that if the law does not respond to the needs of a changing society progress can be stifled. The law must therefore adapt to the speed of technological change. While it is true that many of the general admissibility principles apply to electronic evidence as they do to other types of evidence, because digital evidence is so pervasive, complex, and less readily understood than other types of evidence, it is essential that lawyers litigating in any field develop an understanding of what electronic evidence may be available, what its limitations are, and how it is to be presented in Court. Accordingly, this book is a timely addition to the range of available Evidence texts. It also dispels many of the common misconceptions about the nature of electronic evidence which, combined with the plethora of examples provided, serves to make the subject matter much easier to comprehend and manage.

Brenda Midson*

* Senior Lecturer in Law, University of Waikato.