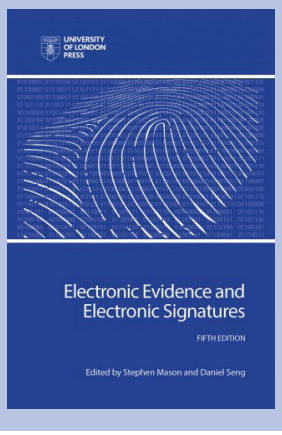
Electronic Evidence and Electronic Signatures (2021) by Stephen Mason and Daniel Seng (eds)

Nicola Monaghan

University of Worcester



Stephen Mason and Daniel Seng (2021) *Electronic Evidence & Electronic Signatures* is published by the University of London Press, OBserving Law Series, priced at £55pb/75hb or as a free pdf.

ISBN 978-1-911507-26-0604

The complexities relating to the treatment of electronic evidence have become increasingly multidimensional as technology has developed. Today, electronic evidence may present in a variety of different sources. Modern day technologies, such as smartphones, tablets, laptops and wearable technologies, which may be connected to the internet via wireless technology or a mobile network, along with the development of cloud computing, the internet of things, the deep web and the dark web, have raised nuanced questions about the reliability and admissibility of electronic evidence.

The new and updated fifth edition of *Electronic Evidence and Electronic Signatures* offers an innovative and comprehensive insight into this area and provides an exhaustive explanation and analysis of the complexities of electronic evidence. Published by the Institute of Advanced Legal Studies for the School of Advanced Studies, University of London Press in 2021, the fifth edition of this book also incorporates Stephen Mason's book on *Electronic Signatures in Law* (Mason 2016), thus offering a detailed

examination and analysis of issues relating to both electronic evidence and electronic signatures.

The editors and authors, Stephen Mason and Daniel Seng, are both leading authorities on electronic evidence. Together with a team of expert contributors, they have compiled 10 unique chapters which deal with a wide variety of aspects relating to electronic evidence, including topics such as the sources and characteristics of electronic evidence and artificial intelligence, hearsay, the presumption that computers are 'reliable', the authentication of electronic evidence, encrypted data and proof (the technical collection and examination of electronic evidence). The book claims to take a traditional approach to the subject and focus primarily on the law in England and Wales, although a number of the chapters provide significant consideration of cases and legislation from other jurisdictions. As such, in some areas, the book offers a comparative perspective (this is most notably, although not exclusively, the case in chapters 5 and 7, which explore these areas in extensive detail). The book is dedicated to Colin Tapper, Emeritus Professor at Magdalen College, University of Oxford, who was pivotal in developing academic scholarship in the law of electronic evidence.

The authors begin each edition of the book with a short vignette. The opening vignette for the fifth edition paints an enlightening, fictional courtroom scene involving a pre-trial application requesting the disclosure of evidence relating to the defendant, Positively Open Ltd's, software system, EarthSkyMeet. This scene serves to contextualize some of the key issues relating to the reliability of electronic evidence. It is upon this foundational depiction of a fundamental procedural process that the chapters in the book are built. It is worth noting that the vignettes used to open previous editions of the text can be found at the end of the book (in appendix 2).

The first chapter of the book provides an overview of the nature of digital evidence. It explores the various sources and characteristics of electronic evidence and artificial intelligence and introduces the reader to key terms and concepts which feature throughout the book. The authors draw attention to the challenges facing legislators in avoiding overly abstract legislation which, while technologically neutral, fails to provide sufficiently precise provisions, and overly specific legislation which quickly falls out of date as technologies advance. The authors offer a helpful and much needed definition of the term 'electronic evidence' which seeks to strike a middle ground. Chapter 2 covers the foundations of electronic evidence. It discusses traditional evidential issues, such as the categories of evidence, means of proof, disclosure, authentication of

evidence, and the best evidence rule in the context of electronic evidence. The chapter outlines the types of electronic evidence that are admissible and considers some areas in which electronic evidence is frequently admitted, including as video and audio evidence in lieu of testimony, or as identification or recognition evidence. The admissibility of computer-generated animations and simulations is also discussed in the context of both civil and criminal proceedings.

Chapter 3 focuses on the rule against hearsay and its relevance in the context of electronic evidence. This is a highly relevant chapter which provides a useful tool for evaluating the admissibility of electronic evidence under the hearsay rule. The authors propose that, first, the *type of device* that is used to produce the evidence should be classified (in accordance with whether human input is supplied) and, second, the *use* that is made of the output of the device should be analysed (on the basis of whether its use is testimonial or non-testimonial). This chapter deals with the admissibility of evidence such as telephone calls, text messages and body-worn camera footage (which has now become an everyday feature of policing), as well as business and other documents. It concludes by drawing upon the importance for lawyers to remain aware of the dangers of admitting hearsay evidence. Chapter 4, which is entitled, 'Software Code as the Witness', illustrates how software code can affect the admissibility of electronic evidence. The author discusses the categorization of digital data and offers an analysis of the evidence falling within each category, drawing upon existing jurisprudence and academic commentary.

Chapter 5 is a significant chapter which challenges the common law presumption introduced by the Law Commission in its Report on *Evidence in Criminal Proceedings* (Law Commission 1997) that computers are reliable. The author critically evaluates the use of a presumption of 'reliability' and explores the nature of software errors. The chapter catalogues a range of errors in a variety of different types of software, including aviation software, medical software, and the software that led to the Post Office Horizon scandal. These topical and interesting accounts are used to challenge the presumption of reliability. The chapter also offers a broader international perspective, drawing upon jurisprudence from Canada, Australia and the United States. The author calls for reconsideration (or a more careful understanding) of the presumption that software code is 'reliable' and emphasises the importance of the disclosure of software code. The chapter concludes with detailed recommendations.

Chapter 6 is about the authentication of electronic evidence. This chapter explores the issues of admissibility and authentication and

draws upon comparative approaches in Australia, Canada and the United States. Central themes, such as identity and integrity, and reliability, are considered, before an examination of methods of authentication. The chapter then considers challenges to the authenticity of evidence. Chapter 7 on electronic signatures, is a new addition to the fifth edition of the book. This substantial chapter is derived from Stephen Mason's book on *Electronic Signatures in Law* (Mason 2016). The chapter begins by explaining the purpose of a signature and the evidential (and other) functions of a signature. There is a discussion about manuscript signatures and the extent to which a manuscript signature can be disputed; however, the focus of the chapter is the electronic signature. The chapter considers the elements of an electronic signature, and the variety of forms in which an electronic signature can manifest are explored (including the use of electronic sound, 'click wrap', personal identification numbers and passwords, typing a name into an electronic document, scanning a manuscript signature, and a biodynamic version of a manuscript signature, such as signing a handheld device) along with the different types of situations and legal fields in which these signatures might be employed and their authentication.

Chapter 8 covers encrypted data and is primarily concerned with the use of encryption to hide material. The chapter considers the disclosure framework in England and Wales and the power to compel the disclosure of a password to break the encryption in order to access encrypted data as set out under Part III of the Regulation of Investigatory Powers Act 2000 and its accompanying Code of Practice (Home Office 2018). The chapter explores the extent to which compelling someone to disclose the key infringes upon the privilege against self-incrimination, and the position in England and Wales is usefully compared to the approaches taken in other jurisdictions namely, the United States, Canada and Belgium.

Chapter 9, entitled 'Proof: the technical collection and examination of electronic evidence', is concerned with the way in which electronic evidence is gathered and handled. The chapter calls for lawyers to understand not just the need to scrutinize digital evidence professionals in relation to their qualifications and conclusions, but also to question the manner in which the evidence was obtained. It explores the importance of the correct handling and gathering of electronic evidence, as well as the preservation and analysis of such evidence, and the preparation of a report setting out the findings and conclusions of the digital evidence professional. The importance of this topic is apparent when considering the useful examples of cases which illustrate various failures and errors made by the police and digital evidence professionals and the consequences, which may very

well be the exclusion of the evidence and the collapse of the case. The final chapter of the book, chapter 10, briefly examines the competence, knowledge and qualifications of witnesses called to give evidence in relation to electronic evidence through an examination of case law.

The book offers a unique and valuable insight into the evidential issues that arise in relation to electronic evidence and electronic signatures. The authors took the decision to make the book available under a Creative Commons licence in order to promote a better understanding of electronic evidence. This enables a wider audience to have access to this authoritative text and to the benefit of the combined scholarship and expertise of the authors. It is a much-appreciated and welcome decision. The electronic open access version of the book is available in the School of Advanced Studies Humanities Digital Library, University of London. The book is also available in hardback and paperback formats. Whilst the book makes a valuable contribution to the field, there could be scope for greater parity in terms of the lengths of chapters in future editions. Overall, this book serves as a valuable practitioner text and will also be of interest to academics and postgraduate students researching in this area.

About the Author

Nicola Monaghan *is a Principal Lecturer at the University of Worcester. She teaches Criminal Law and the Law of Evidence on the LLB. Nicola has been teaching law at higher education institutions since 2001 and has published textbooks on criminal law and evidence:* Criminal Law Directions *(Oxford University Press) and* Law of Evidence *(Cambridge University Press). Her research interests include jury misconduct and the criminal trial, and she has published a wide range of journal articles and contributed to edited collections. Nicola is a non-practising barrister and a member of the Honourable Society of the Middle Temple.*

Email: n.monaghan@worc.ac.uk.

References Cited

Home Office (2018) *Investigation of Protected Electronic Information: Revised Code of Practice* London: Home Office.

Law Commission (1997) *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245) London: HMSO.

Mason, S (2016) *Electronic Signatures in Law* 4th edn London: Institute of Advanced Legal Studies.

Legislation Cited

Regulation of Investigatory Powers Act 2000