BOOK REPORTS

TITLE: **Electronic Discovery and Records Management Guide: Rules, Checklists, and Forms (with CD Rom)**

AUTHORS: **Jay E. Grenig, Browning E. Marean, Matthew J. Stippich and Kelly H. Twigger**

DATE AND PLACE OF PUBLICATION: **United States of America, 2011-2012 Edition**

PUBLISHER: **West, Thompson Reuters**

ISBN number: **978 0 314 60682 2**

This guide to the United States Federal Rules of Civil Procedure urges the reader to take a proactive approach to discovery of electronically stored information. The authors emphasise the need for proper planning in advance, with the emphasis on records management. This guide also recognizes that issues relating to the discovery of electronically stored information that arise in state and federal court, as well as in administrative proceedings. Specific references are made to the 2006 amendments to the Federal Rules of Civil Procedure. The text includes state and federal courts.

TITLE: **Global Policing**

AUTHORS: **Ben Bowling and James Sheptycki**

DATE AND PLACE OF PUBLICATION: **London, 2012**

EDITION: **First**

PUBLISHER: **Sage Publications Limited**

ISBN: **978 1 84920 081 3**

As society becomes networked across the globe, the power of police forces no longer stops at the borders of the nation state. This text illustrates how powerful people have used various mechanisms, especially threats to security, to justify the creation of a new global policing architecture, and how the sub-culture of policing is shaping the world in which we live.

The text considers the 'security agenda' – focused as it is on serious organized crime and terrorism, and how this is transforming policing; the creation of global organizations such as Interpol, regional entities such as Europol, and national policing agencies with a transnational reach; the sub-culture of the 'global cops', blurring boundaries between police, private security, military and secret intelligence agencies; and the reality of transnational policing on the ground, its effectiveness, legitimacy, accountability and future development.

The implications for digital evidence are only too evident, given that legal systems will increasingly have to deal with the acceptance of digital data in legal proceedings. In this respect, control of evidence by the legal system can be an exceedingly powerful riposte to the powers that police forces are gathering globally.

TITLE: **Computer Forensics, Electronic Discovery & Electronic Evidence**

AUTHOR: **Allison Stanfield**

DATE AND PLACE OF PUBLICATION: **Australia, 2009**

EDITION: **First**

PUBLISHER: **LexisNexis Butterworths**

ISBN: **978 0 40 932637 6**

This text examines digital evidence from the moment it is collected its presentation in court. It provides a practical overview, with examples, of computer forensics, electronic discovery and electronic courts in Australia, with a comparison with some overseas jurisdictions.

TITLE: **Dispute Resolution and e-Discovery**

AUTHORS: **Daniel B. Garrie and Yoav M. Griver, with contributions from specialist authors**

DATE AND PLACE OF PUBLICATION: **United States of America, 2011**

EDITION: **First**

PUBLISHER: **West Thomson Reuters**

ISBN: **978 0 314 60448 4**

This publication focuses on professionals engaged in or conducting arbitration or dispute resolution in the context of electronic discovery in the United States of America, including the London Court of International Arbitration. The discussion includes a review of the core issues on electronic discovery and makes recommendations on how to handle these issues in arbitration.

© Pario Communications Limited, 2012

TITLE: **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**

AUTHOR: **Eoghan Casey, BS, MA, with contributions from specialist authors**

DATE AND PLACE OF PUBLICATION: **United States of America, 2011**

EDITION: **Third**

PUBLISHER: **Academic Press, an imprint of Elsevier**

ISBN: **978 0 12 374268 1**

TITLE: **Digital evidence: computer forensics and legal issues arising from computer investigations**

AUTHOR: **Michael J. Hannon**

DATE AND PLACE OF PUBLICATION: **Buffalo, New York, 2012**

PUBLISHER: **William S. Hein & Co, Inc.**

ISBN: **978 0 8377 1689 3**

Both of these texts provide introductory materials to digital evidence that is aimed primarily at digital evidence specialists, but is also a useful source of information for judges and lawyers across the world. Both books take the reader through how computer networks function, how they can be involved in crimes, and how they can be used as a source of evidence. In Eoghan Casey, additional chapters cover networked Windows, Unix, and Macintosh computers, and network forensics. Of the greatest value are the chapters dealing with conducting a digital investigation; handling a digital crime scene; investigative reconstructions with digital evidence; and digital evidence as an alibi.

Professor Michael J. Hannon, who is the Associate Director for Library and Educational Technology at the University of Minnesota, focuses on the United States of America, whilst Eoghan Casey's text includes a broad chapter on substantive crimes that have an electronic evidence component within Europe.

Both books would be useful for lawyer to have on their shelves. The technical discussions are extremely useful, notwithstanding that Professor Hannon restricts himself to referencing US sources and materials in the absence of much excellent work undertaken elsewhere in the world at both national and international levels. However, this is minor shortcoming – his citations of US case law is correct, as opposed to the cases cited in Eoghan Casey, although this is a relatively minor problem that most lawyers should be able to overcome.

It is difficult to understand – in fact it is a struggle to comprehend why both books neglect to cite or refer to in any way the most significant texts on electronic evidence by lawyers, and what lawyers have to say on such important matters as the definition of electronic evidence, for instance. Less forgiving, given that both texts are produced in the US, is that neither refers, at the very least, to George L. Paul, *Foundations of Digital Evidence* (2008) American Bar Association, Chicago. This lacunae is somewhat puzzling, given that this area is directly related to law and evidence – it is as if these two books are the only texts that offer an insight into electronic evidence. That they completely ignore texts on electronic evidence by lawyers can at best be described as odd.

Notwithstanding the disappointing deficiency in references and critical analysis of books on electronic evidence written by lawyers, both these texts deserve a place on the bookshelf.

© Pario Communications Limited, 2012

TITLE: **Electronic Evidence**
GENERAL EDITOR: **Stephen Mason**
DATE AND PLACE OF PUBLICATION:
London, 2012
EDITION: **Third**
PUBLISHER: **LexisNexis Butterworths**
ISBN number: **978 1 40577 987 6**

This book introduces lawyers to the practical concepts of electronic evidence, how it is created, stored and structured, including computer forensics and digital evidence specialists. It covers disclosure, procedural process and admissibility.

The text will help lawyers advise on electronic evidence confidently, with assurance and competently. The text covers a mix of common law jurisdictions, enabling lawyers and judges to be aware of decisions made in other, related jurisdictions.

The text covers:

Sources of digital evidence George R. S. Weir and Stephen Mason
The characteristics of digital evidence Burkhard Schafer and Stephen Mason
Proof: the investigation, collection and examination of digital evidence Stephen Mason and Andrew Sheldon
Authenticating digital data Stephen Mason and Allison Stanfield
Mechanical instruments: the presumption of being in order Stephen Mason
Encrypted data Stephen Mason
Using graphical technology to present evidence Dr Damian Schofield and Stephen Mason
Australia Allison Stanfield, Philip N. Argy and Seamus E. Byrne
Canada Steve Coughlan and Robert J. Currie
England & Wales Stephen Mason, Clive Freedman and Sandip Patel
European Union Stephen Mason
Hong Kong Special Administrative Region, People' s Republic of China Ronald Yu and David Leung
India Ms Manisha T. Karia and Mr Tejas D. Karia
Ireland Ruth Cannon and Catherine Dawson
New Zealand Dr Chris Gallavin
Scotland Iain G. Mitchell QC
Singapore Daniel Seng and Bryan Tan
South Africa Julien Hofman and Justin de Jager
United States of America Joseph J. Schwerha IV, John W. Bagby and Brian W. Esler

TITLE: **Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents**
GENERAL EDITOR: **Jean-François Blanchette**
DATE AND PLACE OF PUBLICATION:
Cambridge, Massachusetts, 2012
PUBLISHER: **The MIT Press**
ISBN number: **978 0 262 01751 0**

This book is not about the burden of proof or the law relating to electronic evidence. The reader must look to legal text books on electronic evidence to understand burdens of proof and the law relating to electronic evidence. However, it is a useful text in discussing the technical issues and policy decisions behind the use of technology that has an effect on electronic evidence.

Jean-François Blanchette is an Assistant Professor in the Department of Information Studies in the University of California, Los Angeles. He takes the reader through some of the technical responses to the authenticity of records in digital format and considers the digital traces that appear, from the technical perspective, not to be sufficiently reliable in terms of guarantees of authorship that enable them to perform reliably as documentary evidence.

The book is also a study of how digital signatures have failed to become integrated into the fabric of electronic networks – unless, that is, people are forced to use them (as in some European and South American countries), or where they are not aware they are using them (as with the chip on European bank cards).

The chapters consist of:

Introduction
Communication in the Presence of Adversaries
On the Brink of a Revolution
The Equivalent of a Written Signature
Written Proof
Paper and State
The Cryptographic Imagination
Epilogue

Of interest is that the author was called upon to take part in the process of advising the French government in relation to electronic signatures, and outlines three examples of systems that were developed in France, using electronic signatures and software products to change physical systems into electronic systems.

This is a technical text that the legal reader will find of interest in understanding the issues, problems and possible resolutions relating to cryptography and software. It is not a legal text, and the potential legal reader should be aware that although the author does admit the concept of 'non-repudiation' is meaningless, he does not elaborate on this sufficiently.

Nevertheless, this is an interesting text that has a slight flaw, in that it sadly fails to reference some significant books on electronic signatures written by lawyers (Lorna Brazell, *Electronic Signatures and Identities Law and Regulation* (2nd edn, Sweet & Maxwell, 2008) [first edition 2004] and Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012)[first edition 2003]). This is a shame, because the lawyers and technicians need to continue to take part in a dialogue in relation to electronic signatures and electronic evidence from their different perspectives.

© Pario Communications Limited, 2012