Canadian Journal of Law and Technology

Volume 17 | Number 1 Article 16

6-1-2019

Digital Evidence: A Practitioner's Handbook by Gerald Chan & Susan Magotiaux

Robert J. Currie
Faculty of Law, Schulich School of Law, Dalhousie University

Book Review

Digital Evidence: A Practitioner's Handbook
by Gerald Chan & Susan Magotiaux
(Toronto: Emond Publishing, 2017)

by Robert J. Currie*

Digital Evidence: A Practitioner's Handbook by distinguished criminal defence lawyer Gerald Chan and former Crown Prosecutor Susan Magotiaux (now Justice of the Ontario Court of Justice) is one of the newer titles in the successful "Criminal Law Series" recently launched by Emond Publishing (under its "Emond Professional" imprint).[1] The goal of the series, says the publisher, is to offer "clear and concise guidance on the practical and procedural aspects of criminal law,"[2] and with this book the authors and publishers have correctly identified an area of need for such guidance.

The challenges that are presented to Canadian litigation by the need to effectively obtain and deal with digital evidence (often referred to as "electronic evidence"[3]) are manifold and reflect, in my view, two obstacles. First, the speed with which digitization has entered society (and particularly our communications via the internet) is outmatched only by the rapidity of change and development in this space. Second, so far as the justice system goes this fast pace must be handled by lawyers, who have variable ability to deal with it. Any casual survey of lawyers, and particularly judges, will reveal some who were called to bar after the introduction of the iPhone X (2017), and others who were called prior to the introduction of the *Canadian Charter of Rights and Freedoms* (1982). A group of professionals with a demographic spread this wide requires solid resources to keep up with developments that affect so profoundly the courtroom process and the evidence led in it.

Happily, *Digital Evidence: A Practitioner's Handbook* is exactly the solid kind of resource needed for criminal practitioners, as it is a concise but thorough and well-written guide through the technical and sometimes complex world of digital evidence. The book is divided into three parts, the first two (Part I, "Search and Seizure" and Part II, "Disclosure") focused on procedure and the third (Part III, "Use of Evidence") on how digital evidence is dealt with in the courtroom.

In Part I the authors helpfully explore the manner in which the Supreme Court's recent jurisprudence on privacy in the context of digitized information

---

* Co-Editor-in-Chief; Professor of Law, Schulich School of Law.

1 Emond Publishing, "Criminal Law Series," online: < emond.ca/professional/criminal-law-series.html >.

2 Ibid.

3 See Stephen Mason, ed., *Electronic Evidence*, 3rd ed (London: LexisNexis UK, 2012).

has changed the landscape of our search and seizure law, followed by specific and detailed treatments of search of devices, access to digital data, and the law around the interception of private communications. In Part II their attention turns to the technical needs and legal requirements around disclosure, with one chapter that specifically focuses on the specialized and sensitive area of internet child exploitation cases. Chapter 7, entitled "Practical Constraints on Crown and Defence," demonstrates the depth of knowledge of these two very adept and experienced criminal practitioners, as well as more generally the usefulness and practicality of this kind of book.

Part III very lucidly explores the admissibility regime relating to digital evidence under the *Canada Evidence Act*,[4] which has been in place for two decades but continues to confound and confuse. This is followed by a review of the probative value of different kinds of digital evidence, with expert technical explanations of such topics as cellphone geolocation, forensic reports, the use of hashtag values on digital images, etc. This section concludes with a short but highly practical chapter on presenting digital evidence in court, both in terms of format of data and the use of experts. Finally, a number of chapters are accompanied by appendices that set out the statutory provisions that are germane to the subject matter of the respective chapters, which is a highly useful feature.

When one writes a book on a highly dynamic topic, the risk is run that parts of the book will become out-of-date in fairly short order. I am sympathetic in this respect to the authors of this book, Chapter 4 of which deals with the interception of private communications and became slightly out-of-date as this book review was being written.[5] Due to the pace of change, Mr. Chan and Justice Magotiaux have created for themselves something of a make-work project, as this book more than many others will require constant revision. As the work itself demonstrates, however, they are more than equal to the task. Long may they update it.

---

4 R.S.C. 1985, c. C-5.

5 On April 18, 2019 the Supreme Court released its decision in *R. v. Mills*, 2019 SCC 22, in which the majority held that online communications between an accused and a police officer engaged in a child luring sting operation did not amount to "private communications" for the purposes of engaging the wiretap provisions of the *Criminal Code*.