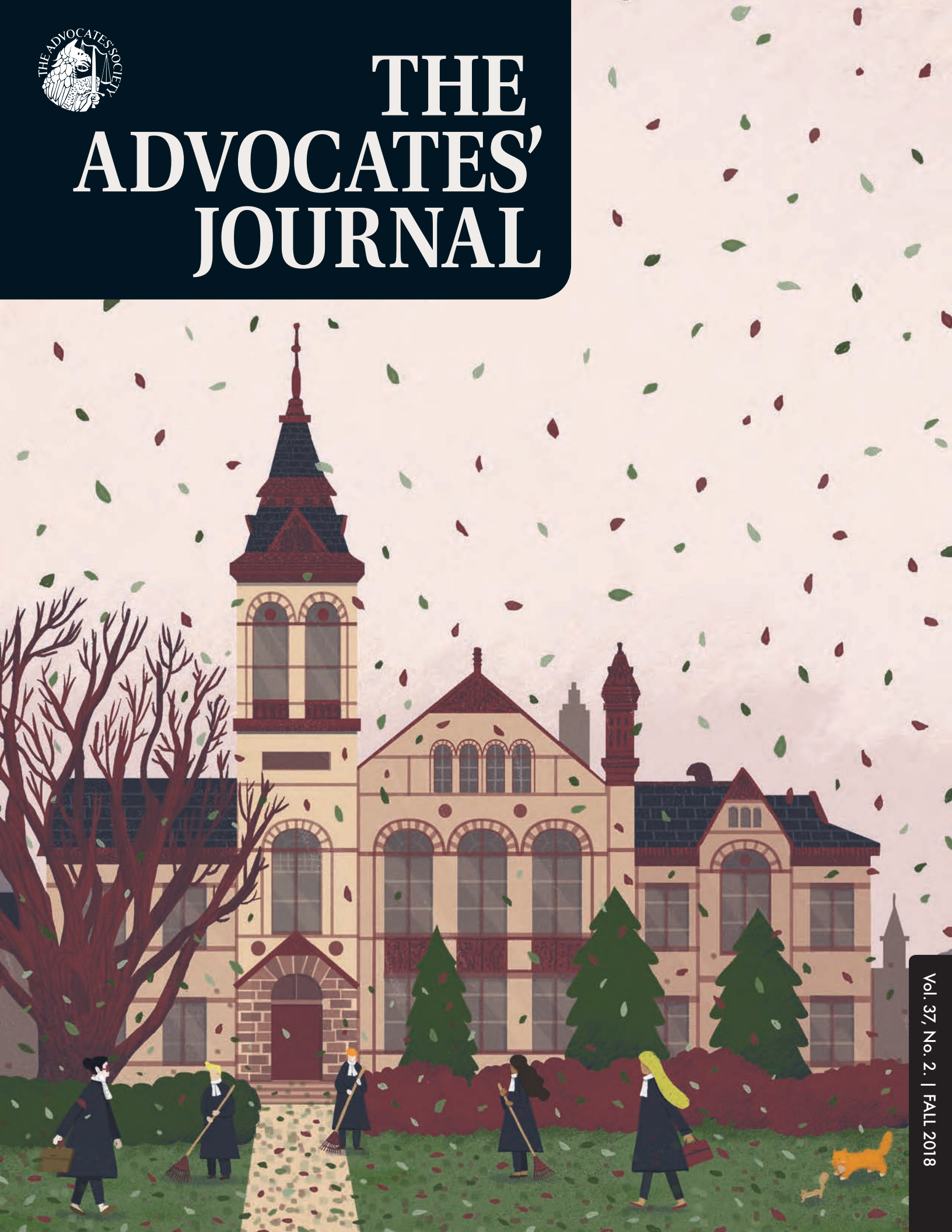
THE ADVOCATES' JOURNAL



Vol. 37, No. 2. | FALL 2018

Advocacy in the information age

Lonny J. Rosen

Gerald Chan and Susan Magotiaux
Digital Evidence: A Practitioner's Handbook
(Toronto: Emond Publishing, 2017; Criminal Law Series, Brian H. Greenspan and Justice Vincenzo Rondinelli, general editors)

For anyone doing trials or hearings in the digital age, *Digital Evidence: A Practitioner's Handbook* is an indispensable aid.

Whether a proceeding is in the criminal, regulatory or civil realm, more and more of the evidence is in digital format: texts, social media postings, electronic copies of videos and photos, medical records, Blackberry PINs – the list goes on. But even as the number of documents in a typical proceeding has increased exponentially, counsel's obligations to marshal the evidence, to address issues of privilege, authenticity, admissibility and relevance, and to assess the probative value of the evidence has not been altered. Not only are counsel challenged to identify, gather and present a greater number of documents than ever before, but the evidence is also increasingly in unfamiliar formats. Where these formats are digital, Chan and Magotiaux have counsel's back.

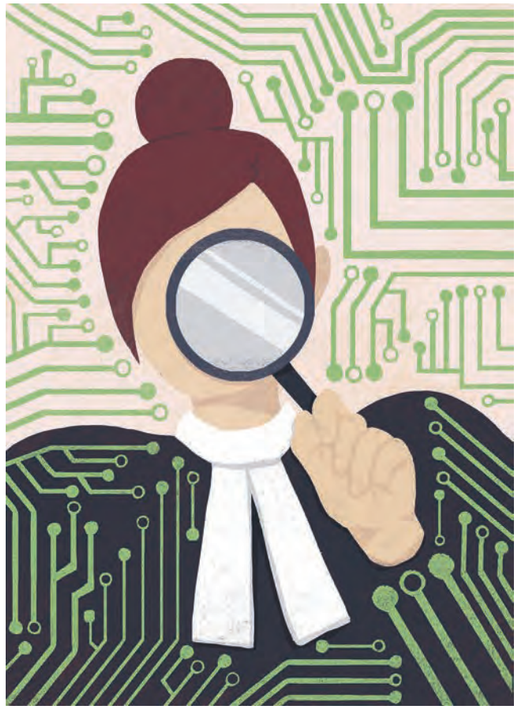
In a foreword to the book, the Honourable Thomas A. Cromwell notes:

> Our justice system depends on advocates to understand the subtleties of a new technology and how it fits in with the general principles established by our courts. Nowhere is skilled advocacy more important than in providing the evidential base and in explaining complex technologies in a digestible way.

Chan and Magotiaux help advocates understand these subtleties by exploring substantive and procedural issues, as well as the underlying principles. The authors discuss the tension between the need for flexibility in the laws of digital privacy, with constantly evolving technology, and the need for certainty in such laws. There is also a tension between the individual's rights and reasonable expectations of privacy and the state's need to lawfully access digital communications. The authors, a leading defence counsel and a Crown attorney, take pains to explore both sides of these debates, making for a text that is authoritative and useful for all counsel.

Chan and Magotiaux begin with explanations of the basic concepts of "reasonable expectation of privacy" and "totality of circumstances" and explain the first principles of privacy law in a manner tailored to counsel who must apply these concepts in submissions involving the rights of their clients, or the state, to access or use digital evidence.

The authors then trace the development of the law regarding privacy and digital evidence, from the Supreme Court of Canada's decision in *R. v. Edwards*, [1996] 1 SCR 128, which sets out some of the factors relevant to the analysis of a person's privacy interest, to later cases that have reframed these factors, articulating and grouping the overarching



concerns. They then explain how courts have applied the traditional factors in privacy and search and seizure analyses, such as ownership, access and control, to the digital world, where the authors advise us to focus on *what* data were seized, not on *where* the machine sat at the time of seizure. Through this approach, counsel can then examine and argue the extent to which data fall within the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (*R. v. Plant*, [1993] 3 SCR 281), a factor that can be determinative of this analysis. The authors note that defence counsel will tend to push as much as they can into that core, while Crown counsel seek to restrict it.

The widest area of conflict, and the focus of much discussion in the jurisprudence, includes defining the precise nature of the digital evidence and the details it reveals, and assessing the reasonableness of the expectation of privacy at issue. The authors note the conflict in modern societal values between the deep concern for privacy and the drive for publicity by recording and showing every minute detail of life in public online forums. These competing desires will be significant issues in the challenges facing digital evidence. The book explores some of the implications of this tension, including the fact that the overextension of online anonymity protection could impede investigation of internet crime, and they caution that recognition of a privacy interest does not create any right to online anonymity and must not impede law enforcement. These are thorny areas of shifting parameters and much debate, which are changing over time to reflect societal values, expectations, awareness and objectives. The book thoroughly explores these challenges throughout.

The book's greatest strength is in its practical approach and tools for counsel. It summarizes the procedural requirements for searches of digital devices, interception of private communications, authentication, and the presentation of digital evidence in court, and excerpts relevant provisions of the *Criminal Code* and the *Canada Evidence Act*.

This book is part of Emond's *Criminal Law Series*, which aims to offer a practical and detailed approach to each topic in the series. The authors do not disappoint in this regard. The book is usefully divided into three parts. Part I, Search and Seizure, will appeal primarily to criminal law practitioners. Part II, Disclosure, is relevant to lawyers who practise criminal or regulatory law. And Part III, Use of Evidence, will be of use to all advocates who are faced with challenges involving digital evidence. The section on search and seizure includes a summary of the law of search warrants and general warrants, searches incident to arrest, exigent circumstances, plain view and consent, all as they apply to digital evidence. Chan and Magotiaux also provide a framework for considering the admissibility of different classes of information, noting that particular factors will be given different weight in the analysis with regard to different classes of digital information.

Email and text messages are perhaps the most frequently encountered digital evidence, and this text explores the "blurred lines" of applying old law to new technologies, including the challenge of examining each party's expectations of privacy in ongoing conversations carried on through digital means. Although written before recent Supreme Court of Canada decisions in *R. v. Marakah*, 2017 SCC 59, [2017] 2 SCR 608, and *R. v. Jones*, 2017 SCC 60, [2017] 2 SCR 696, the book nonetheless examines the state's right to intercept ongoing communications and how this differs from its right to seize copies of historical communications (i.e., those which reside on a computer that could be seized). The authors note that this contemplates seizure of a device which will continue to receive communications, including even messages from an accused's lawyer. In this regard, the authors remind readers of the lawyer's duty to take all reasonable steps to ensure privacy and safekeeping of a client's confidential information and to consider how communication via text could affect that.

After covering the basics, the authors examine some of the special challenges with digital evidence – for example, the application of search and seizure law to data that are increasingly not located on a thing that is seized, but that reside as a string of binary code on multiple servers across the world. That data lack location presents myriad problems for the application of search and seizure principles, including the potentially limitless data that can be accessed and captured through a computer connected to the internet, as well as the fact that seizure of data does not actually reduce a person's ability to access that data.

Recognizing that the reasonable expectation of privacy and the privacy interests at stake in digital data are paramount concerns in determining the state's right to access the data, the authors analyze this issue in the context of regulatory proceedings and contract law, as well as international law (for data that reside outside Canada). The authors provide a practical tool for this analysis in the form of a chart of various types of authorizations and orders available (preservation, production, tracking and transmission of data), their use and the standards required for issuance, as well as the applicable sections of the *Criminal Code*.

Disclosure in the digital age is addressed in Part II. Chan and Magotiaux begin the discussion with the premise that the Crown or regulators have a duty to disclose all relevant information that is not subject to privilege; but they note that, while there is discretion as to the form of disclosure, this is limited. The disclosure must be in a form that is reasonably accessible to the accused or registrant to facilitate the right to make full answer and defence. This is a standard determined by a contextual analysis, balancing the tension between the rights of the accused or registrant and the need for efficient use of resources and to prosecute offences in the public interest. One consideration is the ability of the accused – and their counsel – to access the data, and this imposes a duty of technological proficiency on the part of counsel. A similar consideration is the need to disclose data in a useful format. This may be a searchable PDF document or disclosure of the data in its native format. This poses challenges where software or hardware required to access the data are prohibitively expensive, as the accused must be permitted to fairly check and challenge the analyses done by state examiners. This challenge is particularly acute with forensic examination of data, often done with proprietary, expensive software. In the circumstances, some accommodation must be made.

Protecting sensitive data such as complainants' statements is another problematic issue with disclosure of digital data, particularly with self-represented accused or registrants. The authors recommend that counsel agree to conditions or seek judicial orders to ensure proper protection of the disclosure.

A chapter in the Disclosure section is devoted to practical constraints on the Crown and defence, including undertakings to protect safety and public interests (a precedent is provided); considerations of delay in the post–*R. v. Jordan* era; and the consequences of "over disclosure," including information overload and cost concerns. The authors recommend that the parties look for practical solutions on a case-by-case basis. One practical problem identified is relevant to accessing disclosure in child protection cases: Merely accessing an image on a computer can leave traces of the image on the computer, leaving counsel, Crown attorneys and even judges exposed to potentially serious consequences. A practical, though costly solution is proposed: disclosure of such images on a preloaded freestanding non-modifiable computer, to be returned after the conclusion of the proceedings.

Use of evidence at the trial or hearing is the focus of Part III, and the authors apply the challenges of admissibility (including demonstrating authenticity, the best evidence rule, expert evidence and hearsay) to digital evidence. A chapter on probative value provides a guide to counsel on the use that can be made of digital evidence, including for identification, cell phone geolocation, character and credibility, and forensic purposes. This chapter is replete with checklists of factors to determine uses of digital data and possession of the data.

The book concludes with a chapter on presentation of digital evidence in a trial or hearing, recognizing that the presentation of digital evidence has its own challenges, including format, admissibility, expert evidence and trial fairness.

This text is a must-have for counsel preparing or trying a case that involves digital evidence.