O brave new world that has such books in it!

Jill R. Presser

Nader R. Hasan and Gerald Chan, eds.
Digital Privacy: Criminal, Civil and Regulatory Litigation
(Toronto: LexisNexis Canada, 2018)

In 1990, Justice Gérard La Forest recognized that "the broad and general right to be secure from unreasonable search and seizure guaranteed by section 8 [of the *Charter of Rights and Freedoms*] is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take."[1]

The issue there, in *R v. Wong*, was whether there is a reasonable expectation of privacy inside one's hotel room. The majority of the Supreme Court held that there is. They held that police cannot surveil folks in their hotel rooms unless they have prior judicial authorization allowing them to do so.

The "new" technology at issue in *Wong* was videotaping.

This serves as a measure of how far we have come technologically, and how quickly. In retrospect, Justice La Forest's concern for ensuring that section 8 keeps pace with technological development seems prescient. But even he could not have foreseen the exponential advance of digital communications technology – or the veritable buffet of previously unimaginable options that it presents for agents of the state to peer into our private lives.[2]

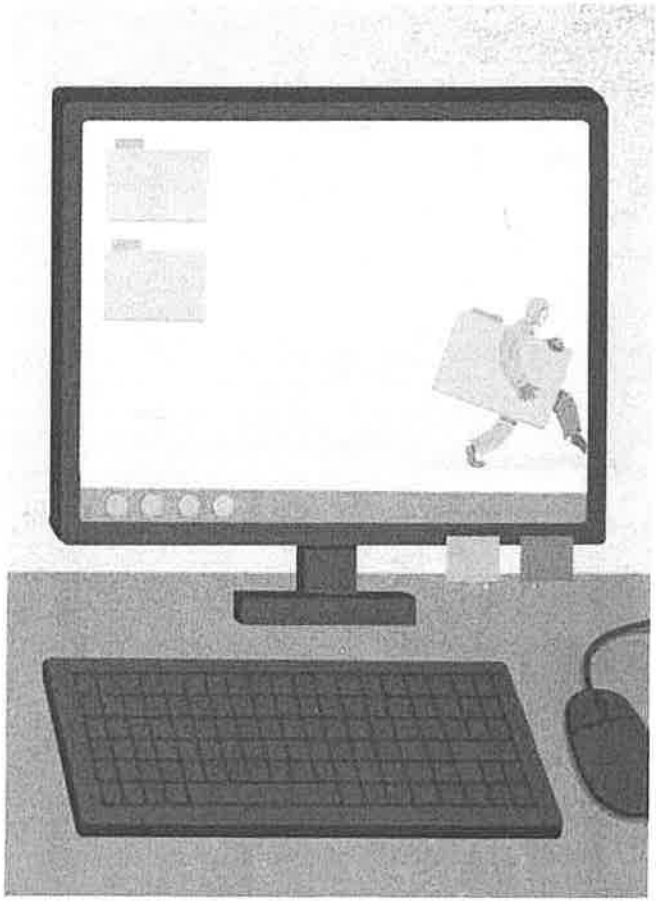
That is because, according to visionary futurist Ray Kurzweil, the rate of technological development is accelerating exponentially. Even the rate of exponential growth is growing exponentially.

Our privacy can now be violated in more varied, insidious and inexpensive ways by the state and its agents, by corporations (think surveillance-capitalism à la Facebook/Cambridge Analytica) and by individuals (see *R. v. Jarvis*) than ever before. And it means that our privacy is less at risk today from these intrusions, by a lot, than it will be tomorrow.

This is why the new book *Digital Privacy: Criminal, Civil and Regulatory Litigation*, edited by Nader Hasan and Gerald Chan, is essential reading.

The book is a thorough manual, fully covering the interdisciplinary legal landscape of digital privacy in Canada. The first section, focusing on privacy rights vis-à-vis the state, contains chapters dealing with searches of our digital devices, searches and seizures of information in the hands of third parties, and search and seizure of private digital communications.

The second section reviews the law around invasions of privacy committed by private individuals and entities. This section includes chapters examining the law on privacy-related crimes; the civil and regulatory consequences of invading another's privacy; and class action lawsuits against those who breach privacy.



The final chapter addresses the rules of evidence dealing with digital data. Although well-written, informative and thoughtful, this chapter arguably does not belong in this book since it is about the admissibility of digital evidence – not about digital privacy. That said, the chapter is useful since we all need to know how to deal with digital evidence. And, although the evidence chapter may not conceptually belong here, neither does it diminish the conceptual coherence of the rest of the book.

In fact, conceptual coherence of privacy law is a central value in this book. In their preface, Chan and Hasan note the importance of an interdisciplinary approach to the law of privacy and their goal of promoting "the continued development of a coherent body of privacy law across different areas of law."

Digital Privacy is a complete guide to litigating privacy claims

in Canada. To fully learn the law of the land about digital privacy, one can read it cover to cover. But the book also works as a research tool. Each chapter is a stand-alone resource, authoritatively covering its own topic.

The book operates on several levels. It tells readers what the law is at present. It also helpfully offers many practical tips to litigators, other jurists and police officers dealing with privacy issues. *Digital Privacy* is a treasure trove of practical advice on key questions. For example: What evidence needs to be called in support of an application for exclusion of evidence? When are wiretap authorizations required, and when will less onerous production orders suffice? And what are best practices regarding digital evidence?

In addition to carefully explaining what the law is at present, *Digital Privacy* tells us how we got here. It describes the initially halting journey of Canadian law to deal with privacy in a digital world where privacy is challenged – and threatened – by the proliferation of digital data trails we create everywhere we go and in everything we do. In Chapter 2 ("Search and Seizure," by Stephen Aylward), for example, the book reaches back to the slow inception of our privacy law journey, it plots our current course and it looks to the American jurisprudence, so we may make comparisons and learn from its experience.

But where *Digital Privacy* really achieves liftoff and distinguishes itself from an anodyne black letter law manual is where it charts a course into the future. The authors identify open questions yet to be determined. Then they propose some answers. (A few of the issues that were undetermined at the time of writing have since been decided. A book such as this one, by its nature, will need updates.)

This is not a purely objective retelling of the law. There is advocacy here. Hasan and Chan acknowledge right off the top, in the preface, that when it comes to privacy, they have opinions on this evolving area of the law. They explicitly endorse a legal path ensuring "that our law of privacy keeps pace with the technological realities of our ever-changing world." They adopt the language of the Supreme Court of Canada in *R. v. Jones*: that Canadians should not be required "to become digital recluses in order to maintain some semblance of privacy in their lives."

In short, the editors and authors have a view, and it is an extremely important one.

New digital media need novel approaches in law to ensure that privacy is protected. The authors of *Digital Privacy* rise to the challenge. They point the way to a radical reimagining of the law to meet the needs of Canadians in the brave new world of emerging technologies.

Notes

1. *R v Wong*, [1990] 3 SCR 36 at para 9.
2. In *Wong*, *ibid*, at para 9, La Forest J cited Brandeis J's prophetic dissenting opinion in *Olmstead v United States*, 277 U.S. 438 (1928). He cited it for its foresightedness about the need for legal protections of privacy to keep pace with the technologically fuelled ability of the state to look into people's private lives. Ironically, La Forest J noted then that Brandeis J could not have anticipated the rate of technological advance between the time of the *Olmstead* decision and the time La Forest was writing in *Wong*.