Canadian Journal of Law and Technology

Volume 14 | Number 2 Article 5

6-1-2016

# Review Essay: Sara M. Smyth, Cybercrime in Canadian Criminal Law, 2nd edition (Toronton: Carswell, 2015)

Christopher D. Ram

# Review Essay:

## Sara M. Smyth, *Cybercrime in Canadian Criminal Law*, 2nd ed. (Toronto: Carswell, 2015)

Christopher D. Ram*

Dr. Smyth's book is ambitious in its scope, seeking to trace the criminology and evolution of information technologies and cybercrime as the basis of current Canadian legislation and jurisprudence. It is intended as a concise student reference text or resource for those who are new to the subject area, studying in criminology and other areas, as opposed to law. A list of concepts and issues for discussion appears at the conclusion of each chapter and there is a glossary of technical (but not legal) terms at the end of the book. It takes a neutral and professorial approach, seeking to identify issues as opposed to expressing opinions, but in the field of cybercrime, this itself involves editorial judgments. It would have been nice to see more of the author's own views, if not on the substantive issues discussed, then at least with respect to which issues and areas she thinks are most important and why.

The book is a concise overview with more detailed analyses in selected areas, and a bit more contextual discussion identifying areas that were not included would also be helpful to its target audience. Experts on information law and cybercrime will turn to more specific and detailed texts on most of the major issues, but students, non-lawyers and others new to the subject area need more context, especially in criminal law. Cases cited are generally limited to decisions based on post-Internet offences, and a number of earlier foundational decisions that shaped the 1985 *Criminal Code*[1] computer crime enactments and subsequent laws are not mentioned. The book is not meant to be a comparative law study, but the development of Canadian law on cybercrime, electronic surveillance and privacy, as well as relevant *Charter*[2] provisions have also been influenced by issues that have arisen—though not always by the judgments rendered—in the U.S. and U.K. and some discussion of this in several areas would have added valuable insight for non-lawyers.

Stylistically, the book is well-written and reasonably well organized, but the effort to keep it short (260 pages) has no doubt led to some difficult editorial decisions about what not to include. It covers fairly well those areas the author has chosen to address, but coverage is uneven, there are some significant gaps in discussions of both criminological concepts and jurisprudence, and the author has been selective in her substantive areas of focus. That is not in itself a bad

---

* LL.B., LL.M. Counsel, Criminal Law Policy Section, Justice Canada. Opinions expressed are those of the author alone.

1 R.S.C. 1985, c. C-46.

2 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (U.K.), c. 11 [*Charter*].

thing, but future editions of the book could profit from an expanded overview of cybercrime, its past, present and future evolution, and some contextual discussion of how the elements included in the book fit into the broader picture. The book is intended to focus on cybercrime as reflected in Canadian criminal law, but the connections between the author's sociological and criminological discussions of what offenders do online, how and why—many of which are very good introductions to the issues she raises—and how these are addressed, or not, by Canadian legislation and case law are a bit uneven. The relationships between child abuse and child pornography activities and Canadian law are well-described, for example, but the discussions of malware and hacking focus on offender activities with little or no explanation of the relevant *Criminal Code* offences.

One of the challenges of explaining cybercrime, especially for educational purposes, is setting out connections between science, engineering, the social and individual behaviours they produce, and the criminological and legal implications of those behaviours. Another is capturing the dynamic nature of the process—how the past nature of technologies and cybercrime has produced the cybercrime we have today and what all of that might suggest about the future. The book deals with most of the important elements in these areas, but it would be much improved if the connections that are so important to understanding the subject matter could be expanded and integrated into many of the specific discussions. It starts with overviews of the technological environment and cybercrime itself. The first is a fairly detailed review of the development of the internet, computers and software as a dynamic process, but the author does not make the connections, explaining how the technological developments she discusses have affected online conduct or how all of this has affected cybercrime.

The overview of cybercrime itself is much shorter than the text discussing technologies, and has omitted some important historical information. The author suggests that the origins of computer crime lie in fictional depictions such as the William Gibson "cyberpunk" stories of the early 1980s, without mentioning that actual crimes involving computer technologies arose at least two decades before that, and that in criminological terms, criminal misuses arose as soon as the technologies themselves created opportunities for those who have access to them. The first Canadian and U.S. federal legislation dates from the mid-1980s, but U.S. state legislatures, which had primary jurisdiction until the inter-state nature of the internet emerged, date from almost a decade earlier. The first law journal dedicated to computer law issues was started in 1978, and at least five books, one U.S. government manual on computer crime, and a number of criminological and legal papers were published in the 1970s. Mr. Gibson's work represents a remarkable contribution to fictional and criminological thought, but he did not invent cybercrime; the offenders did. The first responses to it are found in academic, private sector and government sources, not fictional ones, and as above, pre-1985 incidents, cases and commentaries are critical to

understanding why successive Canadian governments and Parliaments have enacted as they have.

Historical material could be the subject of an entire book, but some mention and footnoting of the sources is critical to understanding the nature and evolution of cybercrime, because elements of the problem predate critical developments such as: the miniaturization of computers; expansions in the speed and capacity of data processing, transmission and storage; and the global explosion in interconnectedness since the Internet became a significant factor in the late 1980s. For example, we now understand that data storage and retrieval technologies have tended to increase risks by concentrating large volumes of valuable or sensitive data in one place. This is evident in the national security leaks of Bradley/Chelsea Manning and Edward Snowden and the many incidents where large data files of personal information have been hacked, but the fundamental problem pre-dates the Internet. It led, for example, to serious physical attacks and data losses from computer centres in the 1960s and 1970s, one of them in Canada, which is why subsection 430(1.1) of the *Criminal Code* addresses damage to data whether it is caused by sophisticated electronic intrusions or dynamiting a building full of file servers.[3]

Some discussions are quite good, but in many there is lack of legal and criminological rigour in discussing specific types of crime or how they fit into Canadian criminal law, and several significant offences, including data-mischief (subsection 430(1.1)) and the illicit possession of devices and passwords (subsections 342.01, 342.2 and 342.1(1)(d)) do not appear to have been considered much if at all.[4] That might in part reflect the paucity of case law, but if so, the lack of prosecutions might itself have been worthy of some comment or discussion. The book is not intended to be an annotated *Criminal Code*, but insofar as it is directed at non-lawyers, it would have been helpful to have listed the statutory provisions in the index or in a table of legislation (there is a table of cases) at the beginning. Some provisions are quoted and discussed in some detail, but others, especially section 342.1 and subsection 430(1.1), the core elements of the original 1985 amendments, are not, and reproducing these either in the appropriate chapters or an additional annex at the end of the book would be a big improvement.[5]

This uneven connection to criminal law is problematic in a book directed at non-lawyers, and more so in the field of cybercrime, where one of the most fundamental policy and legal challenges lies in assessing when pre-existing criminal offences of general application are viable in digital environments and when those environments transform the nature of harmful activities and the harms they are capable of causing to the point where entirely new offences are needed. The discussion of "cyber-fraud", for example, never explains to the

---

3 *Criminal Code*, *supra* note 1, s. 430(1.1).

4 See *ibid*, ss. 430(1.1), 342.01, 342.2, and 342.1(1)(d).

5 See *ibid*, ss. 342.1 and 430(1.1).

reader what the core offence of "fraud" in Canadian law consists of, and then includes a range of other economic crimes that are not fraud variants. "Crimes against banks", for example, are not frauds, but represent a category of offences defined by the victim. The use of so-called "ransomware"[6] is also not fraud, but is rather a form of extortion. Identity-related crimes are unusual in that they have a dual nature defined by motive and victim, and this might usefully have been mentioned: the primary victim, deprived of non-economic interests, is the real person (if any) whose identity is "stolen", and secondary victims are those targeted by other crimes, such as fraud, using the stolen identity. Credit card "skimming" is also not fraud *per se*, but something older than computer fraud and more closely related to identity crime, which is why it is a separate offence in the *Criminal Code*. Another major weakness of this chapter is the failure to distinguish between fraud and theft and to discuss (see below) what can and cannot be "stolen" online. All of that said, the concerns arise mostly from a lack of fundamental and contextual information. The content that actually is included for the most part effectively discusses the offences that are considered, and it is particularly strong in explaining the technological and criminological details of how offenders actually exploit the technological opportunities offered to them.

The various discussions of legislation and jurisprudence raise similar concerns, tending to focus mostly on cyber-specific elements of the *Criminal Code* at the expense of laws of more general application that also form an important part of Canada's legal response to cybercrime. The brief discussion of cyber-espionage focuses on U.S. sources without considering how the Canadian *Security of Information Act*[7] espionage offences would apply in digital circumstances, for example. The discussion of investigative and privacy rights issues (Chapter 10) focuses on the *Charter* and case law based on Part VI of the *Criminal Code*, but the provisions of Part VI itself, which sets out most of the electronic surveillance powers and safeguards on which the cases cited were based, is not mentioned until later in the text. The text does mention both seizure and interception, but does not discuss the differences between the two, or point out that cases such as *R. v. Sanelli*[8] and *R. v. Wong*,[9] which are cited as the basis of basic points of *Charter* privacy law as it applies to seizures, actually arose out of Part VI interceptions. This is not incorrect, but the clarity of the text would be greatly improved by starting with some mention of why communications interception and data seizures are treated differently and then explaining the extent to which constitutional and statutory privacy safeguards apply to each. Canadian and U.S. legislators have traditionally dealt with communications interceptions and electronic surveillance as different and more intrusive (or more

---

6 See, Sara M. Smyth, *Cybercrime in Canadian Criminal Law*, 2nd ed. (Toronto: Carswell, 2015) at 49.

7 R.S.C. 1985, c. O-5.

8 1990 CarswellOnt 77, 1990 CarswellOnt 986, [1990] 1 S.C.R. 30 (S.C.C.).

9 1990 CarswellOnt 58,1990 CarswellOnt 1008, [1990] 3 S.C.R. 36 (S.C.C.).

covert) than physical searches, and whether this distinction will remain viable as technologies converge and investigations in digital environments become more complex and more common is another major unresolved legal and policy issue that could have been identified.

There are also one or two over-simplifications in Chapter 10. The idea that " . . .Parliament now has many methods at its disposal by which it can collect information about us and conduct surveillance. . ."[10] is misleading for non-lawyers and is a rather startling proposition for those of us who actually develop new laws for a living or who work in law enforcement. Parliament does not collect personal information or conduct surveillance. Canada's constitutional rule of law and human rights framework entails laws which are (at least in the case of government proposals) generated by executive experts and proposed by ministers and enacted by Parliamentarians who are for the most part politically accountable. Once enacted, however, any sort of enforcement, and especially the sorts of rights-intrusive investigative measures discussed in this chapter, are a matter for independent law enforcement agencies overseen by independent judges.

One suspects that content distinguishing between what Parliament enacts and what police agencies enforce was mistakenly edited out here and this might seem a small oversight to those new to the area, but the failure to distinguish between executive, legislative and judicial functions and to point out the general requirement that physical or electronic invasions of privacy require, first and foremost, prior and independent judicial approval is a major omission in a chapter discussing these issues. The statutory requirements for prior judicial approval in *Criminal Code* Parts VI and XV are not mentioned, and the decision of the Supreme Court in *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*,[11] which held that invasions of privacy not subject to prior judicial approval were *prima facie* unreasonable under the *Charter*, is cited only on other points. There is a lot of discussion about the use of warrants, but not of what a warrant actually *is* or why they are required. Practising lawyers understand that a search warrant is a judicial instrument that ensures beforehand that informed judicial approval is obtained, and attests that it has in fact been obtained to those subject to the warrant when it is executed, but the book's target audience may not. The actual analysis of judgments on what sorts of privacy rights or expectations apply in respect of various sorts of information, such as locations and data-systems is reasonably good, but the author ought to have pointed out that the judicial review from which all of them arose is itself a constitutional and rule of law requirement. This is also something of a missed opportunity: judicial safeguards have always been a cornerstone of investigative law in Canada, but they are rapidly emerging as a global issue as well. In transnational cases, domestic judges cannot authorise intrusive measures

---

[10] Smyth, *supra* note 6 at 240.

[11] 1984 CarswellAlta 121, 1984 CarswellAlta415, [1984] 2 S.C.R. 145 (S.C.C.).

in another country, and the conventional channels for mutual legal assistance, which include approval by the courts of the state where the data are, are being criticised as too slow for online searches, where exigent circumstances (in which the data will be moved or deleted if not copied immediately) are common.

Opportunities to identify and consider some other issues which currently bedevil the legislatures of many different countries were also missed in the segments discussing lawful access and human rights/privacy issues. One such is the increasing difficulty of ensuring that laws based on physical search and seizure scenarios remain to the extent possible technology-neutral, both in legislative drafting and in recent cases such as the 2013 Canadian Supreme Court decision in *R. v. Telus Communications Co.*.[12] Another is the challenge of distinguishing between the "seizure" of stored data and the "interception" of private communications in transit, which in U.S. and Canadian law generate different expectations and standards of privacy, but which are becoming harder to distinguish in both law and privacy rights policy as a result of technology-convergence.

A third is the vexing investigative and privacy challenges being posed by the extraterritorial storage and transfer of data in "cloud" computing and other multinational network scenarios. The practical challenges facing investigators are prodigious, but the most critical issues for discussion—and not just among students—are the jurisdictional and rule of law ones. Data in the cloud become subject to the laws of whatever country they are stored in or transmitted through, as opposed to those of the jurisdictions in which the people who have privacy interests actually live. What expectations of privacy should Canadians have in respect of their offshore data, and on whose laws should those expectations—and privacy rights in general—be based? If hackers in the Russian Federation access the private personal data of Canadians stored on a cloud server in Sweden, has a Canadian offence been committed in law? If so, as a matter of criminal justice policy and international relations, which country should seek to extradite and prosecute the offenders? These are very much live issues, of concern to federal and provincial privacy watchdogs in Canada and their foreign counterparts, and while a detailed discussion might perhaps have stretched the scope and length of the book too far, identifying them as issues for discussion and referring the reader to other resources would have been useful.

A number of fundamental issues are raised, but the author tends to deal with them on an *ad hoc* basis as incidental to some of the substantive offences being discussed. The result is a smooth narrative flow and readable text, but content which is less accessible and harder to find. There is a good index at the end, but this is a book you read for interest or general class preparation, not a reference source in which to look up facts or issues on demand. The discussion of cloud computing is inexplicably located in Chapter 3, which discusses fraud and identity theft, even though the jurisdictional and practical challenges that cloud

---

[12] 2013 SCC 16, 2013 CarswellOnt 3216, 2013 CarswellOnt 3217 (S.C.C.).

computing and storage pose are more or less the same for most common forms of cybercrime. Similarly, the use of encryption and anonymity applications such as remailers is certainly a major challenge for child pornography and abuse investigators because many paedophiles have developed and shared skills in their use, but as with cloud computing, the basic problems they pose affect the investigation of any kind of cybercrime, not just child sex abuse offences. Apart from making issues harder to find in reference searches, this approach also under-emphasizes the importance some of the more serious issues.

Chapter 4 does contain a good review of legislation and cases dealing with child pornography. This is clearly an area of interest and expertise for Dr. Smyth, and her technical review of how offenders use the internet and various applications and devices is excellent. The only major issue not considered in this segment is perhaps the most fundamental one, at least in criminological terms. We know that data and network technologies have reduced offender risks and transformed child pornography as an illicit commodity for production, trafficking and use. We know that apparent, and probably real, rates of offending have increased as a result. But what does this tell us about the offenders? Unlike some other forms of cybercrime, offending rates are not just determined by changes in opportunity and risk, which are influenced by technological change, but also the intervening factor of sexual attraction to children, which probably is not. She refers at various times to "paedophiles", "child pornography offenders" and "child pornography enthusiasts", but never really discusses the open question of whether the internet has somehow increased the prevalence of paedophilia in our societies, or merely increased the volume of offences and prevalence of paedophile offenders by making it easier for a fraction of the population that was always attracted to children to commit offences they did not commit before data and network technologies made it possible to do so.

Chapter 3 also contains a useful introduction to some of the effects of information technologies on organized crime and *vice versa*, although the working definition of criminal organization that she attributes to a paper by Professor Brenner is actually the United Nations Convention against Transnational Organized Crime[13] a working version of which was also the basis of the Canadian *Criminal Code* definition. The discussion is a good starting point, but mostly focuses on organized crime as an established and known phenomenon and how it has adapted to and used technologies for its traditional activities and goals. Students might also have been invited to consider the more fundamental effects on organization itself. Internet capacity and interconnectedness have had sweeping effects on how human beings organize, communicate and interact in every place and every activity in which we have access to them, and organized crime is unlikely to be an exception. We see entirely new forms of organization among online paedophiles (whose motives and participation often do not involve a "material benefit", at least in the

[13] *Smyth*, *supra* note 6 at 69-70;12-15 December 2000, 2225 U.N.T.S. 209 (entered into force 29 September 2003).

economic sense), and among hackers, who form remote and selectively anonymous organizational structures based on skills, for example. Where traditional organized criminal groups recruit based on valuable skills or unrelated factors such as family or ethno-cultural ties, transient online groups often form spontaneously when individuals with complementary skills find each other. It is perhaps beyond the scope of the book, but the significant effects of the internet on terrorist recruitment, organization and offending might also have been mentioned as an issue.

As mentioned above, the jurisprudence cited is also more limited in scope than one might wish. It focuses mostly on cases based on the post-1985 *Criminal Code* provisions specific to computer-related crimes. These are well-compiled and explained, but the book overlooks some of the earlier cases that establish key concepts on which the legislation was based. These include the Supreme Court of Canada decisions in *R. v. Stewart*[14] on whether intangible information can be "property", and *R. v. McLaughlin*,[15] which distinguishes between the internal workings of a computer system and the external workings of a "telecommunications system", both of which influenced thinking on the 1985 *Criminal Code* amendments and subsequent changes to the law.

*McLaughlin*, which made it clear that computers were a new sort of device and would be so treated by the courts was a major impetus for the enactment of the first *Criminal Code* amendments. The same was true of *Stewart*, which held that copying intangible information could not be "theft", because there was no physical property and therefore no transfer or deprivation of the victim. That case dealt with photocopying, but it applies to digital data, and as courts were forced to grapple with crime in information societies, the same issue arose in Australia (*Croton v. The Queen*, 1967) the U.K. (*Oxford v. Moss*, 1979) and the U.S. (*U.S. v. Seidlitz*, 1978).[16] These sparked a major policy and legal debate among academics and legislators that influenced early computer crime enactments in the *Criminal Code* and elsewhere and that continues to the present day. Subsequent cases such as *R. c. Desroches*, *R. c. Cormier*, and *R. v. Maurer* continue to follow *Stewart,* affirming that pure data are not "property" that can be stolen (e.g. by downloading), but that if a tangible device or document is stolen, the value of the theft takes into consideration the value of the data.[17] The reasons for this, which are fully aired in the judgments in *Stewart* of

---

[14] 1988 CarswellOnt 960, 1988 CarswellOnt 110, [1988] 1 S.C.R. 963 (S.C.C.) [*Stewart*].

[15] 1980 CarswellAlta 316, 1980 CarswellAlta 278, [1980] 2 S.C.R. 331 (S.C.C.).

[16] In Canada, *Stewart*, *supra* note 14; in the U.K., *Oxford v. Moss* (1979), 68 Cr. App. R. 183 (U.K. Div. Ct.); in the U.S. see *U.S. v. Seidlitz*, 589 F.2d 152 (U.S. C.A. 4th Cir., 1978); in Australia see *Croton v. The Queen* (1967),117 C.L.R. 326 (Aus. H.C.A.) and Alex Steel, "Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property" (2008) 30 Sydney L Rev at 575.

[17] *R. c. Desroches*, 1992 CarswellQue 15, 16 C.R. (4th) 182 (C.A. Que.) (upholding theft of device containing information and determining value based on the information content); and *R. c. Cromier*, 2013 QCCA 1068, 2013 CarswellQue 14866, 2013 CarswellQue 11730

the Ontario Court of Appeal (which held that pure information had value and could be stolen) and the Supreme Court of Canada (overturning on that issue), may make sense to judges and legal scholars, but they have become increasingly counter-intuitive to law enforcement, media commentators and criminologists as data have become more extensive and valuable and popular media discussions (as discussed in the preface and introduction) tend to describe unauthorised computer network access by analogy to physical trespass.

The failure to discuss *Stewart* is particularly significant: the 1985 *Criminal Code* amendments were based on the Ontario Court of Appeal judgment that data could be stolen and reflected a Parliamentary decision (subsequently agreed with by the Supreme Court) that data should not be treated as "property". This is why the offence in what is now section 342(1)(a) of the *Criminal Code* focuses on the illicit use of computer time or services as opposed to the taking or copying of content data, and why data-mischief is covered by the parallel non-property offence of subsection 430(1.1) rather than the pre-existing mischief offences. The question of whether damage to data could amount to mischief under section 430 did not arise in Canada before the 1985 amendments foreclosed the possibility, but it was before the courts in the U.K. when the amendments were before Parliament. The eventual result (*Cox v. Riley*, 1986)[18] held that damage to data was damage to the tangible device in which it was stored. This has taken U.K. law in a different direction, but that might also have been mentioned. There have also been extensive academic and governmental discussions about whether data should be treated as property or not and whether the criminal law should be applied to protect digital forms of intellectual property. Those are presumably beyond the scope of an introductory work, but two or three paragraphs reviewing *Stewart* and referring readers to subsequent cases and academic discussions both from the mid-1980s when relevant laws in Canada, the U.K. and the U.S. were all enacted, as well as to more recent discussions, would have added substantial value.

Chapter 9 focuses on questions of jurisdiction and internet governance or regulation, and the examination of the Council of Europe's Convention on Cybercrime[19] (Budapest Convention) and practical aspects of international cooperation and technical assistance/capacity building. This provides a good introduction to the area, although more of the many secondary sources could have been footnoted for those in need of more detail. But the failure to cite and explain the 1985 decision of the Supreme Court of Canada in *R. v. Libman*[20] is

---

(C.A. Que.) and *R. v. Maurer*, 2014 SKPC 118, 2014 CarswellSask 319 (Sask. Prov. Ct.), affirmed 2015 CarswellSask 388 (Sask. Q.B.) (information with no tangible element cannot be the object if theft or conversion); see *Stewart*, *supra* note 14.

[18] (1986) 83 Cr. App. R. 54 (U.K. Div. Ct.).

[19] 23 November 2001, E.T.S. No. 185 (entered into force 7 January 2004) [Budapest Convention].

[20] 1985 CarswellOnt 951, 1985 CarswellOnt 951F, [1985] 2 S.C.R. 178 (S.C.C.) [*Libman*].

another significant omission. The book does point out that an offence can be prosecuted in Canada if any part of it took place here,[21] which is correct, but *Libman* is not referenced as the source of this principle, and its actual scope, which is broader and remains an open issue, is not discussed. *Libman* actually held that any "real and substantial connection" between an offence (as opposed to the offenders or other factors) and Canada would trigger Canadian adjudicative jurisdiction, but only up to the limits of the countervailing comity interests of other states. Concurrent jurisdiction was not in the court's view a problem, but to avoid conflicts, however far jurisdiction was extended, it was held to be "coterminous with. . .comity."[22] This is an important point which distinguishes Canadian law from that of some other countries. *Canada (Human Rights Commission) v. Canadian Liberty Net*,[23] which applies *Libman* to telecommunications scenarios (in that case, call-forwarding) might also have been mentioned.

A related point is that while *Libman* extends Canadian jurisdiction insofar as the application of criminal offences and adjudicative jurisdiction are concerned, the case does not apply to any assertion of enforcement jurisdiction, which under international law requires the consent of the state in whose territory the enforcement takes place. This is a particularly important point for law enforcement readers, because any sort of direct cross-border investigative activity will usually be considered an enforcement act (and possibly a criminal offence) by the affected state,[24] and confusing the principles underlying adjudicative and enforcement jurisdiction is a fairly common mistake with potentially serious consequences.

Overall, the book does provide a good overview of the nature of cybercrime and the challenges it presents, especially in explaining how offender behaviours are related to the nature and evolution of computers and network interconnectedness. Some of the general discussions of the social nature and technological architecture of the internet, "cyberspace" and the digital environments in which cybercrime occurs are also quite good, especially as explanations for students without extensive expertise in technologies or law. Some of the legal content (child abuse and pornography) is also accurate and well-written, but the book does not entirely live up to its title insofar as discussing thoroughly how cybercrime is dealt with in Canadian law. To address that subject properly requires the inclusion of several pre-1985 cases, and much clearer, more complete and more accessible explanations of what the *Criminal Code* and other statutes have to say about cybercrime and whether they address the challenges effectively or not is needed. Cybercrime is a global and

---

21 *Smyth*, *supra* note 6 at 229.

22 *Libman*, *supra* note 20 at para. 76.

23 1988 CarswellNat 388, 1998 CarswellNat 387, [1998] 1 S.C.R. 626 (S.C.C.).

24 See Christopher D. Ram, "Cybercrime" in Neil Boister and Robert J. Currie, eds. *Routledge Handbook of Transnational Criminal Law* (Abingdon, New York: Routledge, 2015) 379.

transnational challenge, and Canadian law has also been developed in consultation with other like-minded countries. The Budapest Convention is discussed in that context, but legislative and case law developments, especially in the United States and United Kingdom, could also usefully be incorporated, especially where they have taken a different approach or consider issues that have not yet arisen in Canada.