Wiretapping Smart Phones With Rotary–Dial Phones' Law: How Canada's Wiretap Law is in Desperate Need of Updating

ANNE TURNER *

"The task of adapting laws that were a product of the 1970s to a world of smartphones and social networks is a challenging and profoundly important one."

Justice Moldaver, *R. v. Telus Communications Co.*

I. INTRODUCTION

When Canada's wiretap law was enacted in 1974, the standard method of communication was a rotary dial phone, attached to the wall within someone's home. Phones the size of credit cards that would be carried in someone's pocket everywhere they went, and that would contain information about someone's entire life were the topic of science fiction. Computers were the size of entire houses and the notion that soon everyone would have at least one computer in their home by which they would be able to send messages to friends around the world and search for reams of information on any topic imaginable was beyond the average person's wildest dreams. As a result, Canada's wiretap law contemplated the electronic eavesdropping on one suspect's land-line at their home or office to others using the same technology. While that was

* LL.B. (2002), LL.M (2016). The views expressed in this paper are the author's alone and do not represent the views or positions of the Public Prosecution Service of Canada or the Government of Canada. Portions of this paper were originally submitted as my Major Research Paper for my LL.M. at Osgoode. I would like to thank my husband, Paul Cooper, and family for their support while completing my LL.M as well as my colleagues at the Winnipeg PPSC office. A special thank-you to Jodi Turner who was invaluable in assisting me with finding obscure articles and cases.

just fine in 1974, it is no longer adequate or usable today. The legislation is so out of date to the point of being technological ancient history.

There are two main dilemmas that law enforcement faces in their efforts to wiretap: one is legislative and the other is jurisprudential. First, Canada's wiretap legislation looks almost exactly today as it did in 1974. While aspects of the *Criminal Code*[1] have been updated and revamped, Part VI of the Code has not kept up with the modern realities of communication. Second, the assessment of an individual's reasonable expectation of privacy often remains based on an analysis that tests whether someone can reasonably expect privacy within a certain location (i.e. a search warrant executed at someone's home). Courts are now being asked to assess a reasonable expectation of privacy in circumstances where police are able to use ever-changing technology to track, intercept, and search individuals or their property. The task of adapting laws that were a product of the 1970s to a world of smartphones and social networks is a difficult but important one. The test of a reasonable expectation of privacy has to be assessed with a more realistic test that incorporates technology and its abilities.

A great number of challenges arise. The simple realities of allowing law enforcement to access and intercept the private and intimate conversations of Canadians are, by their very nature, going to be in conflict with *Charter*[2] principles against unreasonable search and seizure. However, law enforcement needs to keep up with the evolution of increasingly sophisticated and secretive technology, and needs techniques to do so.[3]

Law enforcement officials complain that the criminals' ever-increasing use of technology has impeded the ability of police to effectively investigate crime and they have issued several pleas to legislators and the courts to even the playing field.[4] On the other hand, privacy advocates claim that

---

1 *Criminal Code*, RSC 1985, c C-46, s 183 [*Criminal Code*].

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

3 Yoni Rahamim, "Wiretapping and Electronic Surveillance in Canada: The Present State of the Law and Challenges to the Employment of Sophisticated and Intrusive Technology in Law Enforcement" (2004) 18 Windsor Rev Legal Soc Issues 87.

4 See for example: Canadian Association of Chiefs of Police, Remarks by Chief Constable Jim Chu, "Presentation to Standing Senate Committee – Legal and

digitization has been a boon for state surveillance and they demand that legislators and courts forestall Big Brother's advance.[5]

Canadian wiretap legislation desperately requires amendments based on the practical realities of ever-changing technology. Since technology changes so quickly, it would be next to impossible for legislators to anticipate every possible tool or technique that law enforcement may be able to employ in serious criminal investigations. The wording of legislation should be sufficiently open so as not to limit law enforcement's ability to use new tools.

It remains difficult, however, for legislation to adequately predict all possibilities. Therefore, jurisprudence is also required to play a role. Courts must constantly re-assess how a reasonable expectation of privacy is viewed and analyzed in the face of new technology. What is most difficult is providing consistency in the test to be applied so that law enforcement can have some predictability in how their tools and techniques can be used in compliance with the standards required by the *Charter*, particularly s. 8.[6]

This paper will outline the history of Canadian wiretap law and its early reliance on the American legislation that came before it. It will then examine the current Canadian wiretap legislation of Part VI of the *Criminal Code* and propose several ways in which the legislation can be reformed and clarified. The paper will also address some of the attempts made by Parliament at the modernization of warrant legislation within the *Criminal Code* through the introduction and enactment of the 2014 *Protecting Canadians from Online Crime Act*,[7] better known as Bill C-13.

A review of how the Supreme Court, and some lower courts, have attempted to address an individual's reasonable expectation of privacy in the ever-evolving world of technology will also be examined. There will also be a discussion regarding the need to address the reasonable

---

Constitutional Affairs Bill C-13 Protecting Canadians from Online Crime Act" (delivered 6 November 2014), online: <https://cacp.ca/index.html?asst_id=587>.

5 Kevin Haggerty, "Methodology as a Knife: The Process, Politics and Paradox of Evaluating Surveillance" (2009) 17 Crit Criminol 277.

6 *Charter*, *supra* note 2, s 8. Section 8 refers to the right to be secure against unreasonable search or seizure.

7 SC 2014, c 31 [*Protecting Canadians from Online Crime Act*].

expectation of privacy in situations of new technology differently than courts have traditionally addressed an expectation of privacy in physical spaces. Searches of computers, cellular phones, and the internet encompass very different considerations of a reasonable expectation of privacy than a search warrant at a physical space. An evolved analysis and consideration of reasonable expectation of privacy is therefore required. Courts, however, must provide a consistent and predictable approach so that law enforcement can reasonably assess whether their actions are *Charter* compliant.

Proposed amendments to Canada's current wiretap legislation as well as the principles which should guide courts and legislators in addressing these problems will be offered throughout this paper.

II. HISTORY

A. Canada's History of Wiretapping

Prior to 1974, the law regarding the interception of private communications in Canada was uncertain. While there was not a complete lack of legislation or case law, the law regarding the state's use of interception for law enforcement purposes was minimal. In 1880, the *Act to Incorporate The Bell Telephone Company of Canada*[8] was enacted. The primary purpose of this legislation was not to regulate wiretapping by law enforcement, but to prevent damage to Bell's property and interference with service. The act created "a misdemeanor to intercept messages transmitted on Bell telephone lines."[9]

Canada's development of telephone legislation did not progress until the mid-1950's, through provincial regulation of wiretapping, including the *Manitoba Telephone Act*[10] and the *Alberta Government Telephones Act*,[11]

---

8 *Act to Incorporate The Bell Telephone Company of Canada*, SC 1880, c 67, s 25 (as cited in Hubbard, "Wiretapping", *infra* note 9 at 1.1.1).

9 Robert W. Hubbard, Peter M. Brauti & Scott K. Fenton, "Wiretapping & Other Electronic Surveillance: Law and Procedure", (Toronto: Canada Law Book, 2000), at 1.1.1. [Hubbard, "Wiretapping"].

10 SM 1955, c 76, ss 36 and 37 (as cited in Hubbard, "Wiretapping", *ibid* at 1.1.1).

11 SA 1958, c 85, ss 23 and 24 (as cited in Hubbard, "Wiretapping", *supra* note 9 at 1.1.1).

which both prohibited telephone wiretapping. The aim of these acts remained the protection of telephone lines and phone companies' property, rather than a concern for individuals' privacy.

Many municipal police forces in Canada, including the Royal Canadian Mounted Police (RCMP), have used wiretapping in investigations dating back to the late 1950s and early 1960s.[12] Prior to the enactment of federal legislation, provincial Police Commissions were the only bodies overseeing and regulating the use of wiretapping for law enforcement purposes. An officer who believed that he had reasonable and probable grounds for a wiretap would speak to a supervising officer, who in turn would speak to the Chief of the police force. It was not uncommon, however, for officers to skip the formalities of the process and act on their own without obtaining the approval of, or even advising those higher up.[13] The potential for abuse and a complete lack of any consistency in the process is obvious.

The need for a balancing between law enforcement's use of wiretapping and the privacy interests of individuals became apparent. In 1969, the Ouimet committee[14] made efforts to address privacy concerns regarding electronic surveillance. In their report, they stated:

> The Committee considers that the interest which requires protection is the privacy of conversations taking place under such circumstances as to justify a reasonable belief on the part of both parties to the conversation that such conversation is not subject to interception—in the sense of acquisition of that conversation by others through the use of electronic, mechanical or other devices.[15]
>
> ... federal legislation controlling the use of wiretapping and electronic eavesdropping in law enforcement is required.[16]

---

12 David A. Cornfield, "The Right to Privacy in Canada" (1967) 25 Fac L Rev 103.

13 Nathan Forester, "Electronic Surveillance, Criminal Investigations and the Erosion of Constitutional Rights in Canada: Regressive U-Turn or a Mere Bump in the Road Towards *Charter* Justice?" (2010), 73 Sask L Rev 23 [Forester, "Electronic Surveillance"].

14 Roger Ouimet, Chairman, *Report of the Canadian Committee on Corrections, Towards Unite: Criminal Justice and Corrections*, (Ottawa: Information Canada, 1969) [Ouimet Report].

15 *Ibid* at p 82.

16 *Ibid* at p 83.

Thus, Canada took a step to advance the regulation and legislation of wiretapping by law enforcement and the private sector. The Ouimet committee suggested a legislative scheme which would permit interception under only specific conditions, primarily by law enforcement officials where they had obtained prior judicial authorization.

Parliament responded with the enactment of the *Protection of Privacy Act*,[17] which served to amend the *Criminal Code*, the *Official Secrets Act*,[18] and the *Crown Liability Act*.[19] Initially modelled after the United States' *Wiretap Act*,[20] the most significant change to Canadian legislation was the addition of Part IV.1 to the *Criminal Code*.[21] The legislation aimed to achieve two objectives. First, it aimed to protect private communications from interception, other than in compliance with the statute.[22] Second, in an attempt to balance the first, it attempted to recognize the need to allow law enforcement to intercept private communications in the investigation of serious crime and to be able to adduce that evidence at trial.[23]

In 1985, the *Criminal Code* was revised and Part IV.1 became what is now Part VI of the *Criminal Code*. The original legislative structure remains largely intact today.

B. America's History of Wiretapping

The concepts and wording of Canada's initial wiretap legislation were largely taken from the American legislation and case law that preceded it. The first consideration of wiretap law in the United States was in direct response to the case of *United States v. Olmstead*.[24] The United States'

---

17 SC 1973-74, c 50 (as cited in Hubbard, "Wiretapping", *supra* note 9 at 1.1.1).

18 RSC 1970, c O-3.

19 RSC 1970, c C-38.

20 18 USC, Chapter 119, §§ 2510-22 (1970) [18 USC].

21 Hubbard "Wiretapping", *supra* note 9 at 1.1.1.

22 *R v Welsh* (1977), 32 CCC (2d) 363 at para 12, 74 DLR (3d) 748.

23 *Ibid*.

24 277 US 438 (1928). Roy Olmstead was arrested as a result of an investigation into a huge bootlegging ring in the United States. The United States Supreme Court held, by a narrow 5-4 vote, that telephone conversations were to within the Fourth Amendment (the right to be free from unreasonable search and seizure) and that the police had not trespassed into a constitutionally protected area. See also: Juris

Congress passed the *Federal Communications Act*[25] in 1934. The act created an offence to intercept, divulge, or use any telephone communications.[26] Initially, the Supreme Court interpreted the legislation as prohibiting all wiretapping and excluded any such evidence from federal trials.[27] However, the court's attitude became more permissive in the early 1940's, when they ruled that a defendant could object to the use of wiretap evidence against them, but only if they had been a party to the intercepted communication.[28]

The United States' Congress addressed the issue of electronic eavesdropping with the enactment of the *Wiretap Act*, in *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*.[29] The statute contained four basic elements:

1. Prohibitions against unreasonable surveillance by technological devices; [30]
2. Exceptions for legitimate private use of surveillance devices;[31]
3. A system of court-controlled use of surveillance devices by law enforcement officials in certain cases;[32] and
4. Assorted remedies providing for private and public enforcement of the statutory obligations.[33]

The United States has perhaps the most frequently amended wiretap legislation.[34] Today, the American legislation contains many provisions similar to Part VI of the *Criminal Code*. Wiretap authorizations can only be

---

Cederbaums, "Wiretapping and Electronic Eavesdropping: The Law and Its Implications (1969-1970), 7 Criminologica 32 [Cederbaums, "Wiretapping"].

25 47 USC Chapter 5.

26 *Ibid*, § 605.

27 Cederbaums, "Wiretapping", *supra* note 24.

28 *Ibid.*

29 18 USC, *supra* note 20, § 2515.

30 *Ibid*, § 2511.

31 *Ibid*, § 2512(2)(a).

32 *Ibid*, §§ 2516-2519.

33 *Ibid*, § 2520.

34 Dominique Valiquet "Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia" (2006), Library of Parliament 1.

obtained in relation to a specified list of predicate offences, the list of which has been updated over the years.[35] In their application for a wiretap authorization, law enforcement officials must establish that they have probable cause[36] and "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous".[37] Where the American legislation differs from Canadian legislation, however, is that law enforcement is statutorily mandated to minimize listening to conversations that do not implicate the predicate offences for which they have been granted the wiretap authorization.[38] Commentators note that this provision highlights the tension between privacy rights of individuals and law enforcement's need to effectively investigate crime.[39]

III. CURRENT CANADIAN LEGISLATION AND PROPOSALS FOR LEGISLATIVE REFORM

Part VI of the *Criminal Code* contains six general categories of provisions: definitions;[40] offence-creating and exception sections;[41] application, authorization and procedural sections;[42] evidentiary sections;[43] additional penalties sections;[44] and reporting sections.[45] While some provisions of Part VI have been amended over the years, such

---

35 18 USC, *supra* note 20, § 2516(1).

36 *Ibid,* § 2518(1)(d).

37 *Ibid*, § 2518(1)(c).

38 *Ibid*, § 2518(5).

39 Howard J. Kaplan, Joseph A. Matteo & Richard Sillett, "The History and Law of Wiretapping" (Paper delivered at the ABA Section of Litigation 2012 Section Annual Conference, April 18-20, 2012), online: <http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf>.

40 *Criminal Code*, *supra* note 1, s 183.

41 *Ibid*, ss 184, 184.5, 188.2, 191–193.

42 *Ibid*, ss 184.1–184.4, 185–188.

43 *Ibid*, ss 189–190.

44 *Ibid*, s 194.

45 *Ibid*, ss 195, 196, 196.1.

amendments have not been sufficient to address emerging technology and law enforcement's attempts to keep up with the ability to intercept. In this section, I suggest that several areas of Part VI of the Code are in need of change. Such changes should broadly be ruled by principles of practicality and flexibility. With the constant evolution of communication technology, appropriate legislation related to the interception of communications should not be so specific or rigid as to require constant amendments when new tools or techniques are available to law enforcement. While any amendments must be governed by the fundamental principle of balancing an individual's privacy interests with society's interest of effective law enforcement, the restrictive wording of many aspects of the current legislation should be removed to allow for a more practical, flexible legislative scheme.

A. What constitutes a "private communication"?

At the foundation of the law allowing the interception of private communications is the *Criminal Code*'s long and complex definition of "private communication":

> "private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it; [46]

The key consideration must be whether the originator of the communication had a reasonable expectation of privacy, as discussed in more detail below, and that the communication would not be intercepted by anyone other than the person to whom they were communicating.[47]

---

46 *Ibid*, s 183.

47 As one example: *R v Kyling* 2009 QCCS 3311, 95 WCB (2d) 252. Both accused were placed in a police van. The accused were told that the van was wired and that their communications would be recorded. When the interception of those communications was challenged at trial, the court concluded that the conversation between the accused persons was not private and therefore did not fall within Part VI. It was not reasonable for the parties to expect that their

The basic concept of what is considered a communication was first considered in 1980 when the Supreme Court distinguished between a "communication" and a "conversation".[48] They held that a conversation was properly viewed as a series of communications. A communication was viewed as "the passing of thoughts, ideas, words or information from one person to another".[49] In the case of *Goldman v. R*, the Crown's case depended on a face-to-face conversation between the accused and an associate, who had consented to wearing a recording device to assist the police.[50] The court held that the associate wearing the device had no reasonable expectation of privacy regarding the words he spoke, therefore the admissibility of those words was not subject to Part IV.1.[51] However, the accused, who was presumably not aware that his associate was wearing a recording device, did have a reasonable expectation of privacy regarding the words he spoke, therefore the admissibility of his words was subject to Part IV.1.[52] It made it so that the Crown could only introduce evidence of the words of the person who had consented to the interception of the communication. In other words, only one side of the conversation could be introduced.

This interpretation more recently became relevant in the 2011 decision of *R. v. Carter*,[53] in considering not only how to define the originator but also how to define the recipient. Pursuant to a one-party

---

conversation would not be intercepted by "any persons", or more precisely the police.

48 *Goldman v R*, [1980] 1 SCR 976, 1979 CanLII 60 (SCC). Prior to the *Goldman* decision in the Supreme Court, some consideration of the topic had occurred in lower courts: In *R v Miller & Thomas (No. 1)* (cited in Goldman), it seems to have been considered that the originator of a private telephone conversation was the person who made the call. In *R v Jasicek*, an unreported case of the Supreme Court of British Columbia, cited in Goldman, McKay J., rejected the argument that a conversation must be broken down into its separate communications when making a ruling on the admissibility of certain evidence during the course of the trial. He considered it would involve a "strained and unrealistic interpretation of clear words in the statute".

49 *Ibid* at 995.

50 *Ibid* at 989.

51 *Ibid* at 992–993.

52 *Ibid*.

53 2011 ONSC 6752, [2011] OJ No 6298.

consent authorization, an undercover officer was placed in a holding cell with the accused and a third party.[54] His intention was to record any conversation between the accused and the third party while in his presence. The admissibility of the consent-based interceptions was challenged on the basis that the officer, while present during the communications, was not always the intended recipient of the communications between the accused and the third party.[55] The court held that the statutory definition of "private communication" requires that the court look at who the originator intended to be the recipient.[56] It is not going to be sufficient that someone is simply within earshot of a communication.[57] However, there are particular considerations that can be taken in determining the intended recipient: content of the communication, the location of the interaction, physical proximity of the parties, volume of speech, and physical gestures.[58] In other words, the determination of who will be considered an intended recipient will be contextual and fact-specific.

1. What is considered a "telecommunication"?

The *Interpretation Act*[59] defines "telecommunications" as "...the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system".[60]

Part VI authorizations clearly contemplate the interception of communications while they are in-transit, either a conversation being spoken from one person to another or the transmission of a written message while it is between the originator and the recipient. The definition of telecommunication required the 'emission, transmission or reception' of the content of the communication.[61] This definition leads to

---

54 *Ibid* at para 1.

55 *Ibid* at para 4.

56 *Ibid* at para 32.

57 *Ibid.*

58 *Ibid* at para 33.

59 RSC 1985, c I-21.

60 *Ibid*, s 35.

61 *Ibid.*

the conclusion that a Part VI authorization is not required for the prospective interception of non-oral communications that have not yet been transmitted.[62] Presumably, police could use key-stroke software to acquire the content of communications such as emails or text messages before the writer hit the send button. The fact that the communication has not yet been sent should not afford the writer any less of a privacy interest. In fact, it should perhaps be given greater privacy in that the message may never be sent or shared with others.

2. The difficulty with the inclusion of "in Canada"

In 1974, police could, with reasonable certainty, know where the parties were located during any particular intercepted communication because police would know the exact location of a suspect's land-line telephone or the payphone they were using. Police would have received their wiretap authorization for those particular phones at specified geographical locations. They could say, with certainty, that the intercepted communication was either originated or received in Canada.

Cellular telephones, smart phones, and portable computers have eliminated that certainty. The most obvious example is a cellular phone number, for which the police have a valid authorization to intercept telephone conversations and text messages. Police may be lawfully intercepting telephone communications on that phone number for a suspect who resides in Winnipeg, in the middle of January. While listening to an intercepted communication between the suspect and an unknown person, the monitor hears waves crashing and someone in the background requesting another margarita. The monitor records the conversation in which the suspect instructs the unknown person regarding the delivery of a quantity of cocaine. Subsequent police investigation reveals that the suspect went on a last minute holiday outside of Canada, however continued to use their cellular phone.

With the "in Canada" requirement of the current definition of private communication, this interception would not have been in compliance with the Part VI authorization because of the requirement of the definition that the originator be in Canada or the originator intended the communication to be received by a person in Canada. The suspect in the

---

62 Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008), 12:2 Can Crim L Rev 115 [Penney, "Updating"].

example above does not cease to be a valid target of the investigation and police have not lost their statutory pre-conditions (i.e. reasonable ground to believe) regarding the phone number intercepted pursuant to the authorization. Notwithstanding this, the interception would not be in strict compliance with the legislation. Further, what if the target had been communicating by text message? If police were not aware that he was outside of Canada when the communication occurred, but the interception was challenged at trial with evidence from the accused that he was outside of Canada at the time, would the interception of the communication have complied with Part VI requirements?

The problematic aspects of the inclusion of "in Canada" are expanded even further when police intercept computer-based communications pursuant to a lawful authorization. Internet communications provide not only anonymity of the user, as discussed further below, but anonymity of the computer's location. Emails can originate and be rerouted instantly anywhere in the world.[63] Tech-savvy targets may be able to reroute their internet communications through accounts set up in foreign countries while sitting at a computer in a Canadian home. Are police required to establish the precise location of a laptop or tablet in order to intercept lawfully? That requirement may, in some cases of sophisticated individuals or organizations, be next to impossible and thwart a legitimate and important investigation.

Could a general warrant, pursuant to s. 487.01 of the *Criminal Code*, be used to authorize the interception of private communications when none of the parties are within Canada? This possibility relies mainly on the fact that a general warrant can grant law enforcement the authority to do anything that would otherwise constitute an unreasonable search or seizure, as long as there is no other provision of the *Criminal Code* or other act that would provide for a warrant or order permitting the action they have requested.[64] However, Part VI is meant to be a complete code for wiretapping and a court may view Parliament's preclusion of interceptions outside of the circumstances of the definition of "private communication" to have been intentional.[65] In addition, as exemplified above, the fact that

---

63 Hubbard, "Wiretapping", *supra* note 9 at chapter 15.

64 *Criminal Code*, *supra* note 1, s 487.01(1)(c).

65 Hubbard, "Wiretapping", *supra* note 9 at chapter 15.

a party to the communication is outside of Canada may not have been contemplated by police or may be discovered only in the listening or review of the interception, therefore a general warrant would not have been obtained in advance to make the interception to begin with.

In the United States, courts have dealt with a similar issue by determining where the interception takes place. In *United States v. Luong*,[66] the intercepted phone had a billing address and service provider in the District of California. The governing legislation was clear that the statute conferred jurisdiction on a judge to authorize interception of communications only within the territorial jurisdiction of the court in which the judge was sitting.[67] The judge who issued the order allowing interception was located in another jurisdiction. The court held that the most reasonable interpretation was that an interception occurs where the tapped phone is located and where officers first overhear the call.[68] Therefore, the court determined that the interception took place where the police first heard the communication, which was within the issuing judge's jurisdiction, regardless of where the parties to the communication were actually located at the time of any particular communication.

It is understandable and important that a balance be struck between allowing police to lawfully intercept private communications in their variety of modern forms, and the interest to not allow law enforcement to intercept communications all over the world based on an authorization granted by a Canadian court.[69] However, constraining law enforcement to

---

66 471 F (3d) 1107 (9th Cir 2006), 2006 US Lexis 31752.

67 18 USC *supra* note 20, § 2518(3).

68 The court cited three other decisions that also came to the same conclusion: *United States v Rodriguez*, 968 F (2d) 130 (2d Cir 1992) and *United States v Ramirez*, 112 F (3d) 849 (7th Cir 1997) where the courts held that an interception occurs in the jurisdiction where the phone is located, where the second phone in the conversation is located and where the scanner used to overhear the communication is located; *United States v Denman*, 100 F (3d) 399, 403 (5th Cir 1996) where the court held that the interception includes both the location of the phone and the original listening post.

69 Although beyond the scope of this paper, an interesting discussion of the issues surrounding "in Canada" occurred in *X (Re)*, [2010] 1 FCR 460. There the Federal Court was asked to issue warrants to intercept communications of Canadian subjects while they were outside of Canada. Section 21 of the *Canadian Security Intelligence Service Act*, RSC, 1985, c C-23, specifically allows that a warrant be issued to enable

intercept only communications originated or intended to be received in Canada is no longer realistic with current and emerging technology.

If the requirements of "in Canada" were to be completely abandoned, issues of sovereignty and national privacy protections would clearly arise. The balance would fall much too far to the interests of law enforcement if they were potentially allowed to wiretap anyone, anywhere in the world. If Parliament chose to take the approach suggested in *United States v. Luong*, police again could potentially wiretap anyone, anywhere in the world so long as police were listening on Canadian soil. Perhaps the solution that provides balance between the realities of modern law enforcement and the privacy interests of individuals is to focus on the offence, rather than the individuals being targeted. Requiring that the offence being investigated be occurring "in Canada" would appropriately constrain Canadian law enforcement agencies to wiretap only in investigations of Canadian crime, while allowing them to continue to intercept individuals in an on-going investigation even if they were to travel beyond Canadian borders.

3. Why must the recipient be "a person"?

The definition of private communication continues to present difficulties to law enforcement in requiring that a recipient be "a person". The definition contemplates the interception of communications to which the originator is not in Canada, but a communication "is intended by the originator to be received by a person who is in Canada".[70] Many of our daily tasks and communications no longer involve communication with a person but rather with a machine and some of those communications may assist[71] the investigation of an offence: the interception of phone or internet banking that would assist in a money laundering investigation; the interception of an individual phoning in a Hydro reading for a

---

the Service to investigate, within or outside Canada, a threat to the security of Canada. In the 2009 decision, the court held that it had the jurisdiction to grant the warrant because the Service had shown that the interception of the communications would be carried out from within Canada and controlled by Canadian government personnel.

70 *Criminal Code*, supra note 1, s 183.

71 *Ibid*, s 185(1)(e) sets the standard for the naming of a person as someone the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence.

particular address to establish their connection to a home containing a marihuana grow operation; an individual checking-in for a flight through the airline's website as evidence of drug couriering. If the originator of any of those communications was not within Canada when the communication occurred, and they established that they had a reasonable expectation of privacy (which would not be difficult particularly in the circumstances of phone or online banking), would the interception by police pursuant to a lawful authorization be excluded because the recipient of the communication was not a person? The words "by a person" should simply be removed entirely from the definition. Such an amendment would achieve legislation that is far less restrictive and more in line with the practical realities of modern communications.

B. What is considered to be an "interception"?

The Oxford Dictionary defines the word intercept as "obstruct (someone or something) so as to prevent them from continuing to a destination".[72] In the context of law enforcement's interception of communications, the object is not to prevent the communication from continuing to its destination, but rather to surreptitiously receive a copy or listen into the communication.

Section 183 of the *Criminal Code* defines 'intercept' to include "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof".[73] While such a definition may seem quite straight forward, much jurisprudence has developed as a result, making it significantly more complicated.

The discussion of what constitutes an intercept in the context of non-oral communications first started in the United States in the 1994 decision of *Steve Jackson Games, Inc. v. United States Secret Service*.[74] The sole issue on appeal was whether the seizure of the computer that contained private emails that had been sent to an electronic bulletin board, but not yet retrieved by the recipient, constituted an interception by law

---

72 *The Oxford English Dictionary*, online: <http://www.oxforddictionaries.com/definition/english/intercept>, "intercept" (accessed October 28, 2015).

73 *Criminal Code*, *supra* note 1, s 183.

74 36 F (3d) 457 (5th Cir 1994) [*Steve Jackson Games*].

enforcement.[75] The court held that this did not constitute an interception because the government's acquisition of the contents of the communications was not contemporaneous with their transmission. They drew a substantial distinction between interception communications such as emails and accessing communications that were in storage.

The discussion continued, however, in 1998 with the decision of *United States v. Smith*.[76] An employee had guessed the voicemail password of another employee, listened to a message and recorded it.[77] The message was eventually turned over to the U.S. Securities Exchange Commission investigators, because the message indicated criminal activity.[78] The Court, in this case, expanded the definition of intercept. They held that the word intercept entails actually acquiring the contents of a communication, as opposed to access which merely involves being in a position to acquire the contents of a communication.[79] Therefore, given that the content of the voicemail message had been listened to and recorded in this case, it was an interception.

The Canadian approach to defining the word intercept much more closely resembles the approach taken in *Steve Jackson Games* than in *Smith*. As early as 1975, the Alberta Court of Appeal defined intercept as follows: "In at least, its primary sense the word intercept suggests that there must be an interference between the place of origination and the place of destination of the communication."[80]

In 2007, the Supreme Court of British Columbia applied the reasoning from 1975 and answered the question of whether police acquiring emails that had arrived at their destination constituted an interception.[81] The Court held that there was a fundamental difference between the surreptitious interception and recording of messages, and simply searching through stored messages that had been sent, received and

---

75 *Ibid* at p 460.

76 155 F (3d) 1051 (9th Cir 1998) [*Smith*].

77 *Ibid* at para 7.

78 *Ibid* at paras 7–8.

79 *Ibid* at para 25.

80 *R v McQueen* (1975), 25 CCC (2d) 262 at para 8, [1975] 6 WWR 604.

81 *R v Giles* [2007] BCJ No 2918 (QL), 2007 BCSC 1147.

stored at their destination.[82] To constitute an interception, it must occur contemporaneously with the communication itself. Therefore, the court concluded that acquiring emails from a BlackBerry device, after the arrest of the accused, did not constitute an interception within the meaning of Part VI.[83]

The Superior Court of Justice in Ontario then tackled a similar question in *R. v. M.(S.)*[84] in 2012. The court held that in order for communications to fall within the sphere of Part VI, they must be intercepted contemporaneously.[85] The court, however, had difficulty with the inclusion of the word 'acquire' in the definition, given that it might suggest that the seizure of a communication at any point in time would fall within the meaning of intercept.[86] Justice Nordheimer went on, however, to conclude that when one reads Part VI as a whole, it is clear that there is an implicit requirement that the communication be seized contemporaneously with it being made.[87]

With the Supreme Court of Canada's decision in *R. v. Telus Communications Co.*,[88] the definition of intercept has become significantly more complicated and has raised questions about the traditional view that an intercept must be contemporaneous with the communication. Members of the Supreme Court were split on whether the seizure of text messages, pursuant to a general warrant, was invalid because the seizure involved the interception of private communications and should therefore have been made pursuant to a Part VI authorization.

Police had obtained a general warrant which named two Telus customers and required Telus to provide the text messages of those two customers for a subsequent two-week period.[89] Telus was required to produce the information of all text messages sent or received by these

---

82 *Ibid* at para 34.

83 *Ibid* at para 74.

84 [2012] OJ No 2833, 2012 CarswellOnt 7857.

85 *Ibid* at para 20.

86 *Ibid*.

87 *Ibid*.

88 2013 SCC 16, [2013] 2 SCR 3 [*Telus*].

89 *Ibid* at para 8.

customers, on a daily basis, as well as "any related subscriber information."[90]

Justice Abella, writing for herself, Justice LeBel and Justice Fish, concluded that such a seizure should be governed by Part VI and that the general warrant was unlawful. She rejected the traditional notion that an interception had to be contemporaneous, saying that text messages are private communication and, even if they were being stored on the service provider's system, the prospective production required a Part VI authorization. She emphasized that it was the prospective nature of the order that was problematic, and that stored communications were to remain unaffected by this decision.[91]

Justice Moldaver, writing for himself and Justice Karakatsanis, chose to dodge the question of the definition of intercept. He preferred to resolve the appeal on the basis that the investigative technique used by police was "substantively equivalent" to an intercept and therefore a general warrant was not available.[92] However, he did highlight the difficulties that are presented by attempting to use dated legislation to resolve modern legal dilemmas in the area of communications:

> In approaching the matter as I have, I am not unmindful of the need to address the risks to privacy posed by the digital age. The task of adapting laws that were a product of the 1970s to a world of smartphones and social networks is a challenging and profoundly important one. But the resolution of whether what occurred here was or was not, strictly speaking, an intercept is unnecessary, in my view, because there is a narrower basis for decision that guards against unforeseen and potentially far reaching consequences in this complex area of the law.[93]

---

90 *Ibid* at para 9.

91 The debate regarding stored communications was clearly left open when, at paragraph 15, Justice Abella wrote, "We have not been asked to determine whether a general warrant is available to authorize the production of historical text messages, or to consider the operation and validity of the production order provision with respect to private communications. Rather, the focus of this appeal is on whether the general warrant power in s. 487.01 of the Code can authorize the *prospective* production of future text messages from a service provider's computer. That means that we need not address whether the seizure of the text messages would constitute an interception if it were authorized after the messages were stored."

92 *Telus*, *supra* note 88 at para 52.

93 *Ibid* at para 53.

Adding to the discussion, Justice Cromwell, writing for himself and Chief Justice McLachlin, rejected Justice Abella's interpretation of the definition of intercept. He went back to the traditional notion of an interception involving the contemporaneous seizure of on-going communication. He worried that, with Justice Abella's broad interpretation of intercept, police would be required to obtain a Part VI authorization any time they sought to get access to the content of a private communication.[94] He further expressed concern about the temporal aspect that was introduced by Justice Abella's decision. He noted that Justice Abella's approach depends on the fact that the acquisition of the content of the communications in question was an interception if the acquisition was authorized prospectively.[95] The result is that the police may obtain exactly the same information, however on different statutory

---

94 *Ibid* at para 155. "Moreover, if, as my colleague Abella J. maintains (at para 37), "[a]cquiring the substance of a private communication from a computer maintained by a telecommunications service provider" constitutes an interception, then wiretap authorizations may well be required for a host of searches that are clearly not contemplated by Part VI of the *Code*. Police may well have to obtain a Part VI authorization any time they wanted access to the content of private communications, no matter when the message had been sent or whether it had been received or stored on the recipient's device. For example, on a broad reading of "acquire" police seizing e-mails on a Blackberry device would be engaged in an interception because they are acquiring the content of private communications. Similarly, a person authorized to search a computer system as contemplated under s. 487(2.1) would need a wiretap authorization to seize copies of personal communications stored on those computers (including, for example, e-mail messages and stored copies of Internet chats). This approach would run counter to a line of cases in which Canadian courts have found that search warrants are sufficient to allow police to access documents and data stored on a computer: See e.g. *R. v. Cole*, 2012 SCC 53 (S.C.C.), at para. 73; *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241 (Ont. C.A.), at para. 33; *R. v. Bahr*, 2006 ABPC 360, 434 A.R. 1 (Alta. Prov. Ct.); *R. v. Cross* [2007 CarswellOnt 9108(Ont. S.C.J.)], 2007 Can LII 64141, at paras. 25-27; *R. v. Little* [2009 CarswellOnt 8024 (Ont. S.C.J.)], 2009 CanLII 41212, at para. 154; *R. v. Tse*, 2008 BCSC 906, [2008] B.C.J. No. 1766 (B.C. S.C.), at para. 198; *R. v. Weir*, 2001 ABCA 181, 281 A.R. 333 (Alta. C.A.), at para. 19. If the phrase "acquire a communication or ... the substance, meaning or purport thereof" is given a broad meaning, stored private communications that have long been accessible to police under ordinary search warrants or production orders would fall under Part VI."

95 *Ibid* at para 157.

preconditions, depending on the timing of their request.[96] This would include situations in which police obtained a search warrant pursuant to s. 487 of the *Criminal Code* to search a computer seized from an accused. They would be required to obtain a Part VI authorization before viewing the content of any communications on the device. While it would, perhaps, be easy enough for police to delineate that they were not allowed to view items clearly marked as email messages on the computer, would they be able to review documents that could be letters written in a word processing program? Would they be forestalled from viewing internet search histories for the concern that a message sent through social media might fall under a definition of private communication?

Since the decision in *Telus*, many lower courts have been left to wrestle with the effect on the admissibility of intercepted or acquired communications. In *R. v. Croft*,[97] the Court of Queen's Bench of Alberta held that the decision in *Telus* precluded the use of production orders to obtained stored communications. The police had obtained a production order under s. 487.012 that required telecommunication service providers to produce all incoming and outgoing call details and text messages for particular phone numbers listed in the order. The order covered a specific period of time which ended on or prior to the date of the order, therefore the request was for retrospective messages that were stored on a Telus server.[98]

In challenging the constitutional validity of the production order provision of s. 487.012, the accused argued that although *Telus* did not decide the precise issue raised, it should apply equally to the acquisition of text messages already sent, and being stored on a server.[99] They argued that if, as in *Telus*, the order obtained by the police allowed for the acquisition of text messages recorded by a telecommunication service provider, it should properly be an order pursuant to Part VI.[100] The trial judge concluded that when Justice Abella's reasoning from *Telus* was applied to

---

96 *Ibid.*

97 2013 ABQB 640, [2013] AJ No 1231 [*Croft*].

98 *Ibid* at para 7.

99 *Ibid* at para 27.

100 *Ibid.*

the question of whether the acquisition of previously recorded text messages constituted the interception of private communications, the necessary conclusion is yes.[101] Thus, the trial judge found that the production order obtained by the police that authorized the interception of private communications was insufficient.[102] They should properly have obtained an order under Part VI, therefore having to establish the rigorous statutory requirements.

Although the *Croft* decision has not yet been applied outside of Alberta, if the reasoning set out is extended then it may result in the conclusion that police can only obtain stored communications pursuant to a Part VI authorization. Not only would that conclusion require that police obtain a Part VI authorization when seeking to obtain information from telecommunication service providers, but also to situations where police seize a computer or smart phone pursuant to a search warrant and seek to review text or email communication on the device. This conclusion would seem to add an additional hurdle to investigation than was set out by the Supreme Court's decision, also from 2013, in *R. v. Vu*.[103]

Vu clearly set out that computers and similar technological devices, such as smart phones, require different rules than traditional searches. Police are required to obtain specific pre-authorization to search such devices, given their substantial privacy interests.[104] The police will have to satisfy the authorizing justice that there are reasonable grounds to believe that the computer itself will contain the things for which they are looking.[105] Would the *Croft* decision then add that, if the police want to look at communications stored on the computer or other device, they are required to obtain a Part VI authorization? Such a conclusion does not seem logical upon a reading of *Vu*, where the court contemplated and addressed a full search of a seized computer's files.

If a computer or smart phone is lawfully seized by law enforcement, whether incident to arrest or pursuant to a search warrant, police should

---

101 *Ibid* at para 43.

102 *Ibid* at para 66.

103 2013 SCC 60, [2013] 3 SCR 657 [*Vu*].

104 *Ibid* at para 2.

105 *Ibid* at para 3.

not have to comply with the pre-requisites for a wiretap authorization (that the search be related to an offence listed under s. 183, that police establish investigative necessity, that the application be brought by a Crown agent, and that the order be granted by a judge of a Superior Court). Such rigorous pre-conditions are relevant and necessary in the balancing of privacy interests and effective law enforcement in the context of intercepting private communications prospectively. When a device has already been seized lawfully or the messages sought have already been stored (as opposed to a contemporaneous interception while the message was in transit), such a high threshold tips the balance too far to the interests of privacy and will stymie legitimate law enforcement efforts.

The opposite conclusion from *Croft* was reached by the Ontario Superior Court of Justice in 2014 in *R. v. Carty*.[106] Police had obtained text messages of the accused over a defined period of time prior to the order being made from his telecommunication service provider. Like in *Croft*, police had obtained a production order pursuant to s. 487.012.[107] The accused argued that police should have obtained a Part VI authorization.[108] Acknowledging the decision of the Alberta Court in *Croft*, the trial judge in *Carty* held that the *Telus* decision did not control the outcome of the matter before the court.[109] He held that *Telus* applies only to requests by police to acquire private communications prospectively and that it was clear that Justice Abella had confined her findings to such circumstances.[110] The trial judge concluded that the decision in *Telus* should not be understood to have "changed the law" regarding "the appropriate method of judicial authorization for the acquisition of historical, saved personal communications."[111]

The *Telus*, *Croft* and *Carty* decisions have raised an important and complex discussion that can and should be resolved by Parliament. The definition of intercept must be amended to clarify this temporal quandary

---

106 2014 ONSC 212, [2014] OJ No 6081 [*Carty*].

107 *Ibid* at para 4.

108 *Ibid*.

109 *Ibid* at para 48.

110 *Ibid* at para 49.

111 *Ibid* at para 57.

in particular. If it is Parliament's intention to require that police obtain a Part VI authorization for all future communications, it should be made clear in the legislation. Given the slim and divided majority decision in *Telus*, Parliament should step in to clarify expectations. As Professor Penney suggested in 2008, the definition of intercept should be amended to clarify that a Part VI authorization, or as he calls it a "super-warrant", should only be required for the prospective capture of communications content (defined as communications that do not yet exist at the time of requesting the warrant).[112] This could be accomplished by simply amending the definition to read, "listen to, record, or acquire a communication *that has not yet occurred or does not yet exist* or acquire the substance, meaning or purport thereof." If police seek to access the content of communications that already exist, and is identified to be stored at a location, whether a home computer, server or some other identifiable place, they should obtain a regular search warrant or production order.

C. Is the list of offences for which a wiretap can be granted unworkable?

A Part VI authorization cannot be obtained by police for just any offence. As set out in s. 183, the term offence is limited to a list of particular offences mainly under the *Criminal Code*, *Controlled Drugs and Substances Act*,[113] or a variety of other acts containing criminal offence provisions.[114] A catch-all for any criminal organization or terrorism offence is also included within the definition. Although the intention of Parliament initially was to limit Part VI authorizations to only the most serious offences, such as murder, treason and drug trafficking, the list of offences has grown significantly through a series of amendments.

---

112 Penney, "Updating" *supra* note 62 at 130.

113 SC 1996, c 19.

114 A huge variety of offences under other Acts are also included: *Bankruptcy and Insolvency Act*, *Biological and Toxin Weapons Convention Implementation Act*, *Competition Act*, *Corruption of Foreign Public Officials Act*, *Crimes Against Humanity and War Crimes Act*, *Customs Act*, *Excise Act, 2001*, *Export and Import Permits Act*, *Immigration and Refugee Protection Act*, *Security of Information Act* and *Trade-marks Act*.

In addition, there are several glaring omissions to the list of offences. Although police can obtain a Part VI authorization for a murder investigation, they cannot if the offence under investigation is manslaughter. Police can obtain a Part VI authorization for an investigation into the possession of a weapon obtained by the commission of an offence,[115] with a statutorily required minimum punishment of one-year if prosecuted by indictment. However, no authorization is obtained for the offence of possession of a firearm with ammunition.[116] Possession of a firearm with ammunition required a minimum punishment of three years on a first offence,[117] which suggests that Parliament viewed it as a serious offence.

The list included under s. 183 has become so long that its limiting effect to only the most serious offences no longer exists. Parliament should amend s. 183 to allow an application for a Part VI authorization to be made for any offence under the acts as listed. The safeguard of the requirement of investigative necessity and the catch-all requirement that an authorization only be granted where it would be in the best interests of the administration of justice to do so,[118] will eliminate applications for authorizations for minor or trivial offences. In addition, the gatekeeping function of the Crown agent and the practical realities of the enormous costs to law enforcement agencies to implement a Part VI authorization, would not allow for Part VI applications for relatively minor offences.

IV. Areas in Which Some Modernization has Occurred – Bill C-13

Parliament has not remained completely idle in attempting to modernize the warrant provisions of the *Criminal Code* to deal with evolving technology. Some progress was made, although not without

---

115 *Criminal Code*, *supra* note 1, s 96.

116 *Ibid*, s 95.

117 The mandatory minimum that was prescribed by Parliament was struck down in *R v Nur*, 2015 SCC 15, [2015] 1 SCR 773. However, this still shows Parliament's view of the seriousness of the offence.

118 *Criminal Code*, *supra* note 1, s 186(1)(a).

criticism, with the coming into force of Bill C-13[119] on March 8, 2015. The creation of a variety of new types of warrants, and the updating of outdated warrants that had become of little assistance to law enforcement, was achieved. What remains to be seen is whether these new warrants will survive *Charter* scrutiny when, undoubtedly, some if not all will be challenged.

A. Preservation Demand – s. 487.012[120]

Police can now make a demand, without prior judicial authorization, requiring a person to preserve computer data in their possession or control. The demand can be made when an officer has a reasonable suspicion that computer data within the person's possession or control will assist the investigation of an offence. The demand expires after 21 days, when the offence under investigation is one which is alleged to have occurred in Canada, and 90 days when the offence alleged is under the law of a foreign state. The officer who makes the demand can also impose any conditions the officer deems appropriate, including specific conditions that the content and existence of the demand not be disclosed. Once one demand is made, the officer may not make another demand to preserve the same computer data in connection to the same investigation.

Given the transitory nature of computer information, Parliament's attempt to ensure that police have the ability to ensure that information relevant to an investigation is preserved is an important modernization of the warrant provisions of the *Criminal Code*. What remains to be seen from potential challenges to such a demand is whether an appropriate balance has been struck between that aspect of society's interest in the ability of police to obtain such information and an individual's privacy interest in computer data. While limiting the duration of a demand to 21 days for a domestic investigation requires that police move quickly to obtain an order to obtain the information, allowing police the unfettered discretion to impose any conditions they see fit may be ripe for challenge, depending on conditions imposed. Further, unlike a preservation order, as discussed below, there is no requirement that the police establish that they made the demand in anticipation of seeking a preservation order or other warrant to

---

119 *Protecting Canadians from Online Crime Act*, *supra* note 7.

120 *Criminal Code*, *supra* note 1, s 487.012.

obtain the information. This has the potential for abuse in demanding that individuals or organizations preserve computer data unnecessarily, potentially for as long as 90 days.

B. Preservation Order – s. 487.013[121]

The use of a preservation demand by police clearly contemplates that they will move to obtain a preservation order from the court with due haste. Upon introduction of Bill C-13, the preservation order was described as a "do-not-delete" order.[122] A preservation order, issued by the court on the basis of an officer's reasonable suspicion that an offence has been or will be committed and the computer data will assist in the investigation of the offence, serves to extend the timeframe during which a person must preserve computer data within their possession or control to a maximum of 90 days from the making of the order. The section further requires that the officer has applied or intends to apply for a warrant or other order to obtain a document that contains the information.

Some protection exists beyond what is required in a preservation demand, in that such an order is judicially authorized and requires that the officer show a warrant to obtain the information is, at least, intended. Such provision alleviates the potential that individuals or, more likely service providers, will be required to needlessly preserve and store computer data unnecessarily.

C. Tracking Warrants – s. 492.1[123]

Prior to the amendments brought to s. 492.1 of the *Criminal Code*, police could obtain a tracking warrant on the basis of a reasonable suspicion that information relevant to the commission of an offence could be obtained through the use of a tracking device. Police were authorized to install, maintain and monitor a device in or on any thing, including a thing carried, used or worn by any person. In reality, this provision was most often used to install a tracking device on the vehicle of a suspect in an investigation. The section allowed police to install a device that would

---

121 *Ibid*, s 487.013.

122 House of Common Debates, 41st Parl, 2nd Sess, No 025 (7 November 2013) at 1535 (Hon Peter MacKay).

123 *Criminal Code*, *supra* note 1, s 492.1.

allow them to track the location of an individual or a thing, however did not contemplate police being able to acquire such information without the need for them to actively install a device.

The amendments brought by Bill C-13 sought to modernize the section by allowing police to obtain an order for tracking information within devices already in the possession of a target, such as GPS on a cellular phone. The amendments also brought distinctions to the type of tracking warrant that police can obtain. While the standard remains one of reasonable suspicion, Parliament attempted to provide clarity to the modern realities and capabilities of tracking technology. Now an officer may obtain an order that allows police to install and monitor a tracking device to obtain data about either transactions or movements of a thing, including but not limited to a vehicle. An officer may also obtain authorization to obtain data identifying the location of "a thing that is usually carried or worn by the individual" that will assist the investigation.[124] This subsection clearly contemplates the acquisition of data from a cellular phone, or other device, that is already in the possession of the target.

These amendments are an important modernization of tracking warrants because they address the practical realities of how law enforcement can track individuals. The new provisions provide law enforcement with the ability to effectively use modern technology already possessed by almost everyone, but with the necessary balancing of the requirement of prior judicial authorization.

D. Warrant for Transmission Data – s. 492.2[125]

While the focus is often placed on an individual's reasonable expectation of privacy as it relates to the content of private communications, questions remain regarding the ability of law enforcement to obtain "envelope information" without a warrant. As described by Professor Penney, "envelope information" includes the addressing or other information accompanying a communication that is analogous to information that could be obtained from an unopened

---

124 *Ibid*, s 492.1(2).

125 *Ibid*, s 492.2.

letter.[126] Similar to subscriber information, envelope information is not as intimate as information regarding the content of a communication, but may still reveal a great deal about a target of the inquiry. The identity of the persons or organizations with whom the target regularly communicates, the frequency, duration and timing of communications, and the physical location of the communicators may all be of interest to investigators.

The *Criminal Code* did not make reference to information such as envelope information until 1993. Courts were divided on two questions: (1) whether envelope information constituted a private communication and therefore should be governed under Part VI, and (2) whether such information was included in an individual's reasonable expectation of privacy.[127] Those questions were largely resolved with the enactment of s. 492.2, allowing for an application for a warrant for a number recorder. At the time, police could apply for a warrant allowing for the installation and monitoring of a number recorder, which provided police only with information identifying or recording a telephone number or the location of a telephone from which a call originated, was received or was intended to be received.

The amendment of s. 492.2, with Bill C-13, allowed for the modernization of the section to a warrant for a transmission data recorder, rather than only a number recorder. Such warrants now allow the court, based on reasonable grounds to suspect, to issue a warrant allowing the installation and monitoring of a transmission data recorder. "Transmission data" is defined as data that relates to functions of dialing, routing, addressing or signaling; allows for information regarding the type, direction, date, time, duration, size, origin, destination or termination of a communication; and does not reveal the substance, meaning or purpose of the communication.[128] This greatly expands the information that police can receive in this regard. Rather than the limited information that could be received with a number recorder warrant, police are now able to obtain

---

126 Steven Penney, "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 SCLR (2d) 505 [Penney, "Digitization"]; Penney, "Updating", *supra* note 62 at 19.

127 Penney, "Updating", *ibid* at 143.

128 *Criminal Code*, *supra* note 1, s 487.011.

more fulsome information that realistically addresses the type of information that would be helpful to an investigation involving electronic communications.

V. EVOLVING TECHNOLOGY AND THE ANALYSIS OF S. 8 OF THE *CHARTER*

While the provisions for warrants often used as part of a wiretap investigation have undergone updates, the core wiretap authorization provisions remain stuck in the 1970's. Those core provisions of Part VI need to be modernized to remain practical and useful to law enforcement in their efforts to investigate serious, sophisticated crimes.

A second part of the puzzle is equally relevant and necessary. Beyond the issues of wiretap legislation, one must examine the jurisprudence that has developed around an individual's reasonable expectation of privacy. New tools and techniques used by law enforcement must be assessed according to concepts of privacy that have become outdated and inflexible. Courts must formulate an approach that provides consistency with historical concepts of an individual's reasonable expectation of privacy, while being flexible to new tools and techniques that emerge and become available to law enforcement.

At its inception, Part VI (Part IV.1 as it then was) of the *Criminal Code* was intended to be a complete and comprehensive scheme to address the lawfulness and admissibility of intercepted private communications. However with the enactment of the *Charter* and its evolving case law, additional considerations have emerged. Part VI of the *Criminal Code* now addresses the issues regarding the lawfulness of interceptions and s. 8 of the *Charter* governs the admissibility to the evidence gathered as a result of the interceptions.[129] Answering the question of whether a private communication was lawfully intercepted under the rules of Part VI is no longer determinative of the admissibility of the evidence. The court must consider s. 8 of the *Charter* and all of its required analysis.

In addition to calls for legislative reform, the ever-evolving use of technology by criminals and by law enforcement raises questions of whether the established doctrine of analysis for s. 8 of the *Charter* is

---

[129] Hubbard, "Wiretapping" *supra* note 9 at chapter 15.

capable of evaluating the reasonableness of technological searches and an individual's reasonable expectation of privacy in relation to a huge variety of modern devices and applications. A consideration of an individual's reasonable expectation of privacy is essential given that it is the point at which any judicial oversight begins.[130] Failure to establish a reasonable expectation of privacy leaves an accused without standing to challenge the actions of law enforcement, thereby leaving no possibility of remedy.

The first case of "new" digital technology and s. 8 of the *Charter* arose in *R. v. Plant*.[131] After an anonymous tip, police contacted the local electricity company and requested information from their customer database.[132] That information was used in support of an application for a search warrant. The accused argued that police had invaded his reasonable expectation of privacy in obtaining the information from the electricity company. The court held that the information obtained was not sufficiently "personal and confidential" to attract a reasonable expectation of privacy, given that it did not reveal any intimate details of the accused's life.[133]

By 2010, the technological abilities of law enforcement advanced quite significantly from getting billing information from the electricity company. In *R. v. Gomboc*,[134] police asked the electricity company to install a digital recording ammeter (DRA) on the power line connected to a particular house about which they had received information of a marihuana grow operation. The electricity company voluntarily complied and the DRA provided police with detailed information about the electricity consumption at the house. Again, the primary consideration in evaluating the use of this new technology was whether the accused had a reasonable expectation of privacy in the information the device could reveal to law enforcement.[135]

---

130 Mathew Johnson, "Privacy in the Balance – Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8" (2011-2012) 58 Crim LQ 442.

131 [1993] 3 SCR 281, 1993 CarswellAlta 94 [*Plant*].

132 *Ibid* at paras 2–3.

133 *Ibid* at para 27.

134 2010 SCC 55 at para 1, [2010] 3 SCR 211.

135 *Ibid*.

The majority of the court held that the DRA did not invade the accused's reasonable expectation of privacy, but they were divided in their reasons for that conclusion. Justice Deschamps, also writing for Justices Charron, Rothstein, and Cromwell, held that although the DRA produced more fine-grained measurements than the billing information obtained in *Plant*, it did not reveal intimate details of a household's activities.[136] Justice Abella agreed in the conclusion, but wrote that it was mainly because of the regulatory aspect of the analysis. Had it not been for the fact that a customer was required to expressly request confidentiality of the information, she would have found that the accused had a reasonable expectation of privacy.[137] For her, the information inside the home was presumptively protected by an expectation of privacy.

Chief Justice McLachlin, writing a dissent on behalf of herself and Justice Fish, held that a DRA allows for informed predictions about probable activities in the home that, although not conclusive, could provide useful private information to law enforcement.[138] The average consumer who signed up for service of the electric company could not be expected to be aware of a complicated regulatory scheme that allowed for disclosure of certain information to law enforcement.[139] They concluded that the search was not authorized by law, and that the accused's s. 8 *Charter* rights were consequently infringed.

As early as the *Plant* decision in 1993, the Supreme Court demonstrated a shift had to occur away from the considerations of a reasonable expectation of privacy that had traditionally been undertaken in determining one's expectation of privacy in a place.[140] Questions such as whether someone was present at the location at the time of the search and one's possession and control of a physical space did not necessarily fit in an analysis of whether an individual had an expectation of privacy in information they were sending out into the world. The Court stated that one must consider the type of information sought by police and whether it

---

136 *Ibid* at para 14.

137 *Ibid* at paras 82–83.

138 *Ibid* at para 124.

139 *Ibid* at para 139. This makes it seem as though ignorance of the law (or here the regulatory scheme) is permissible.

140 *Plant*, *supra* note 131.

contained intimate details of an individual's life.[141] They considered whether an individual willingly or voluntarily put that information out into the world or, by legislation, had not opted out of disclosure of the information.[142] A move toward the concept of privacy in information, rather than in a place, emerged to deal with evolving technology.

A. Computers and Cellular Phones

The Supreme Court's consideration of the increasing digitization of information quickly moved to technologies that are far more common to all Canadians, with the consideration of one's reasonable expectation of privacy in a search of computers or cellular phones.

With the evolution of technology and the Court's understanding of new technologies, the interpretation of a reasonable expectation of privacy has evolved. For example, when first considering issues surrounding the interception of cordless telephones, some courts held that communications on such devices were not protected by Part VI because of a lack of a reasonable expectation of privacy given the ease with which they could be intercepted, for example with a well-placed scanner.[143] Similarly, with the evolution of cellular phones from early car phones to today's smart phones, courts have continued to re-assess the level to which an individual has a reasonable expectation of privacy. In early jurisprudence on the subject of cellular phones, a Quebec trial judge held that the accused did not have a reasonable expectation of privacy in a cellular phone conversation because, "the ordinary user of a cellular telephone knows or ought to know that the communication transmitted by means of such a device is likely to be intercepted by a person other than the person to whom it was intended".[144] Today, an individual can clearly expect to have a reasonable expectation of privacy in his or her cellular phone conversations or text messages. This presents difficulties to law enforcement in that, while conducting an investigation, they have to attempt to predict the expectation of privacy that will be attributed to one

---

141 *Ibid* at para 20.

142 *Ibid* at paras 21–22.

143 Penney, "Updating" *supra* note 62 at 6; *R v Penna*, 1997 CarswellBC 2914, [1997] BCJ No 3014.

144 *R v Solomon*, 1996 CarswellQue 3084 at para 5, 110 CCC (3d) 354.

device or another. The principles of consistency and predictability are lacking when law enforcement is left to guess at whether the tool or technique they hope to use in a serious criminal investigation is going to be in compliance with s. 8 of the *Charter*.

1. Computers

The evolution of technology and an increasing understanding of computer technology has clarified and solidified the way in which courts will view an individual's expectation of privacy. In the 2010 case of *R. v. Morelli*, Justice Fish commented that it would be difficult to imagine a more intrusive, extensive, or invasive search of one's privacy than the search and seizure of one's personal computer.[145] In his dissent, Justice Deschamps emphasized technology's capacity to facilitate communication of information and exchange of material in infinite quantities instead of stressing the digitization as a threat to privacy.[146]

Since the decision of *R. v. Cole*[147] in 2012, the Supreme Court has made it abundantly clear that computers are going to be treated differently than any other device when it comes to a s. 8 analysis. Computers contain a vast quantity and variety of information therefore the magnitude of information and communications that can be retrieved from them may sometimes exceed what can even be obtained as a result of a Part VI authorization.

In *Cole*, the court unanimously held that there is a very robust expectation of privacy attached to computer data. However, it is tempered by a number of factors. The most significant of those factors was whether the computer in question was at one's workplace or home.[148] The computer in question was provided to the accused by his employer, who could seize and search the computer at any time pursuant to its workplace policies and practices. While that led to a reduction in the accused's reasonable expectation of privacy, it did not extinguish it altogether.[149] The authority of the employer to search and seize the computer did not

---

145 2010 SCC 8 at para 2, [2010] 1 SCR 253.

146 *Ibid* at para 114.

147 2012 SCC 53, [2012] 3 SCR 34 [*Cole*].

148 *Ibid* at para 8.

149 *Ibid* at para 9.

give law enforcement the same search and seizure authority. The court held that the employer could certainly advise law enforcement of their discovery of illegal material on the computer; however police still required a warrant before they could seize the device.[150]

The Supreme Court continued to stress that computer searches are to be treated very differently than traditional searches of places with their decision in *R. v. Vu*.[151] Not only are computers to be treated differently, the Court held that to search a computer the police must have specific authority, even if that computer is found in a place for which police have a valid search warrant or other judicial authorization.[152] The Court effectively deemed a computer to be a distinct place in and of itself. Their reasoning was based primarily on the fact that a computer can be distinguished from a filing cabinet or a briefcase in that it may contain information that users cannot control or may not even be aware they possess.[153] Additionally, computers may act as a gateway to information beyond the physical location of the device or the contents of it. If officers were executing a search warrant at a particular building, they would only be authorized to search the area defined by the warrant and the contents of that location.[154] When connected to the internet, computers open up to an almost infinite amount of information stored anywhere in the world.[155]

The decision in *Vu* highlights the evolution of the Court's analysis of a reasonable expectation of privacy with emerging technology and their understanding of it. They noted that the general principle was that a warrant to search a place would include the authority to search spaces and receptacles within the named place.[156] However they found that that general principle had to be reconsidered when dealing with computers.[157] The particular nature of a computer requires that there be a specific

---

150 *Ibid* at para 73.

151 *Vu*, *supra* note 103.

152 *Ibid* at para 64.

153 *Ibid* at paras 24, 41, 44.

154 *Ibid* at para 44.

155 *Ibid*.

156 *Ibid* at para 39.

157 *Ibid*.

assessment of whether a search of the contents of the computer is justified. The Court concluded that:

> only a specific authorization to search a computer found in the place of search ensures that the authorizing justice has considered the full range of the distinctive privacy concerns raised by computer searches and, having done so, has decided that this threshold has been reached in the circumstances of a particular proposed search.[158]

The decision in *Vu* begs the question of whether Parliament should enact a specific type of search warrant for computers or if the traditional search warrant pursuant to s. 487 will suffice? The Court did not go so far as to hold that a traditional search warrant would be inadequate. However, given the clear language that computers are to be treated differently, perhaps the current legislation is not truly appropriate. A s. 487 search warrant allows an issuing judge to authorize the search of a "building, receptacle or place".[159] While Justice Cromwell clearly treats a computer as a distinct place in *Vu*, it would make far more sense to provide for specific and particular authority for the search of a computer within a distinct section. Such a section, whether a new section or treated as a sub-section to the current s. 487, could address the particularities cited by the Court in *Vu*. This would include the provisions allowing the authority to reproduce and print computer data as currently allowed by s. 487(2.1) and s. 487(2.2), provisions for whether a computer must be disconnected from the internet or a network while being searched,[160] and address potential limiting conditions for the execution of the warrant as contemplated by the court.[161] Such provisions would provide a balance between an individual's high expectation of privacy in a computer, with the highly probative value of what may be found on a computer. Also,

---

158 *Ibid* at para 47.

159 *Criminal Code*, *supra* note 1, s 487.

160 The ability to expand a search to an indefinite number of places was cited as a concern and a distinguishing factor of computer searches. This could be either addressed as a particular provision that a computer is not to be connected (so as to keep the search distinct to the device named in the warrant) or as a potential limiting conditions to be considered by the issuing judge or justice.

161 The court rejected the concept of the issuing judge or justice mandating the manner of search for all warrants however did not rule out the imposition of limiting conditions.

such provisions would provide predictability to law enforcement so they would be aware of the boundaries and parameters of computer searches.

2. Cellular phones

In 1985, there were 6000 wireless subscribers in all of Canada.[162] In 2000 that number increased to 8,731,220 subscribers.[163] In the second quarter of 2015, the number had grown to 28,586,472 subscribers, or 80% of the Canadian population.[164]

The Supreme Court in *Vu* specifically stated that they no longer saw a distinction between the considerations relevant to computers and those relevant to similar forms of technology, such as cellular phones. They recognized that the evolution of cellular phones has resulted in phones that have capacities and capabilities equivalent to computers and thus should be treated no differently,[165] however specifically chose to stay away from any disruption to the law as it related to a computer or cellular phone searched incident to a lawful arrest.[166] Therefore, there remained confusion about whether a cellular phone found on a suspect pursuant to a lawful search incident to arrest, could be searched by police without a warrant.

The Supreme Court attempted to resolve that confusion with its decision in *R. v. Fearon*.[167] The Court held that a modified power to search incident to arrest included the power to search a cellular phone. The majority specified that police must take detailed notes of what was searched, and why, to ensure that such a search was truly incidental to arrest.[168] They held that the scope of the search must be tailored to the

---

162 Canadian Wireless Telecommunications Association, "Mobile Wireless Subscribers in Canada" (March 25 2002), online: < http://www.cwta.ca/wp-content/uploads/2011/08/SubscribersStats_Q4_00.pdf>.

163 *Ibid.*

164 Canadian Wireless Telecommunications Association, Facts & Figures, "Wireless phone subscribers in Canada" (2015), online: <http://www.cwta.ca/wp-content/uploads/2015/08/SubscribersStats_en_2015_Q2.pdf>.

165 *Vu*, *supra* note 103 at para 38.

166 *Ibid* at para 63.

167 2014 SCC 77, [2014] 3 SCR 621 [*Fearon*].

168 *Ibid* at paras 4, 82. The Court attempted to clarify that the search must be founded on a lawful arrest, be truly incidental to that arrest and be conducted reasonably (see para

purpose for which it is being conducted.[169] In other words, an officer cannot search through an entire phone on the basis of the search being incident to arrest. They must confine their search to certain areas or items on the phone that have the necessary link to the purposes for which a prompt examination of the phone is permitted. The police must also show that a valid law enforcement objective would be stymied or significantly hampered if they did not have the ability to promptly search a cellular phone incident to arrest.[170] This factor has significantly changed the law in relation to a search incident to arrest, when it comes to a cellular phone; in other circumstances (such as a search of pockets or immediate physical surroundings), police search for any additional evidence of the offence for which the accused was arrested.

The majority's decision in *Fearon* constituted a move toward removing any bright line rules concerning the search of technological devices. The onus was placed on law enforcement to articulate why their actions fit within the existing search rules and why their actions were reasonable.

Nevertheless, Justices LeBel, Abella and Karakatsanis argued in the dissent that a bright line rule *should* be established. Their position was that searches of personal digital devices cannot be conducted pursuant to the common law power of search incident to arrest and that, given the extremely high expectation of privacy, only judicial pre-authorization can provide a sufficient balance between law enforcement's objectives and the unique privacy interests of the information contained on such devices.[171] They were of the view that the safeguards and conditions imposed by the majority's decision were not sufficient to protect such a significant expectation of privacy.

In some ways the decision of the majority of the Court in *Fearon* is in conflict with their decision in *Vu* just over a year earlier. While the majority in *Fearon* allows police to conduct a limited search of a cellular phone incident to arrest in the appropriate circumstances, *Vu* is in line

---

58). Arguably, it is not extremely helpful in guiding law enforcement officers who are attempting to understand what the court will view as a search incidental to an arrest to clarify by saying that it must be 'truly incidental to arrest'.

169 *Ibid* at para 76.

170 *Ibid* at para 80.

171 *Ibid* at para 105.

with the dissent in Fearon, allowing police only to search a computer when they have specific judicial pre-authorization to do so. Perhaps through the evolution of subsequent case law circumstances will arise where courts find that a limited search of a computer will be allowed in exceptional circumstances where a valid law enforcement objective would be stymied or significantly hampered by delaying a search. However, as the law seems to stand now, such an argument would be counter to the findings in *Vu*.

B. The Internet

As the internet continues to evolve, more new challenges are presented for the application of the provisions of Part VI. Questions such as where the communication originates, whether the originator and/or recipient of the communication are in Canada, should authorities be allowed to access encrypted private communications, and when an individual's expectation of privacy is reasonable while online, continue to expand and contract in case law specific to the internet.

In 2012, 83% of Canadian households had access to the internet at home.[172] Approximately 69% of those connected households used more than one type of device to go online.[173] While laptops and desktop computers remained the preferred type of hardware in those households, the use of wireless handheld devices largely increased from 35% in 2010 to 59% in 2012.[174] Using the internet to communicate by a variety of methods is prevalent in Canadian society as well. In 2012, two-thirds of Canadians who used the internet accessed social networking sites such as Facebook and Twitter.[175] In 2010 only 24% of internet users used the

---

172 Statistics Canada, "Canadian Internet Use Survey 2012" (27 November 2013), online: <http://www.statcan.gc.ca/daily-quotidien/131126/dq131126d-eng.htm>.

173 *Ibid.*

174 *Ibid.* Not surprisingly, a huge amount of households in urban areas (80% of metropolitan areas and 80% of agglomerations) had home internet access, with 75% of households outside of those areas. Almost all households in the top income quartile (household incomes of $94,000 or more) had internet access.

175 Statistics Canada, "Individual Internet Use and e-Commerce, 2012" (28 October 2013), online: <http://www.statcan.gc.ca/daily-quotidien/131028/dq131028a-eng.htm>.

internet to make audio or video calls, which rose to 43% in 2012.[176] Interestingly, the use of the instant messaging through the internet dropped approximately 7% during that same time period, perhaps because of the variety of other messaging options, such as text messaging or communicating through social media sites.[177]

When assessing an individual's reasonable expectation of privacy on the internet, some unique questions arise including whether legislation should require service providers to facilitate the decryption of communications and where an internet communication is intercepted.

1. Should authorities be allowed to intercept encrypted private communications?

It is clear from the statistics regarding internet usage that a huge number of Canadians are using the internet in a variety of ways to communicate. However, depending on the methods or programs used, the internet often does not provide any assurances that those communications will remain private. In fact, many communications over the internet come with an explicit warning that they may, at best, not be secure or, at worst, be subject to interception.[178]

An entire industry has become devoted to the encryption of the internet and of communications, and its use has become widespread. "Encryption" was defined by the American 9th Circuit Court of Appeals as:

---

176 *Ibid.*

177 *Ibid.*

178 Hubbard "Wiretapping" *supra* note 9 at chapter 15. As Judge Fletcher of the 9th Circuit Court of Appeals noted in *Bernstein v United States Deptartment of Justice*, No 97-16686 (9th Cir 1999) [*Bernstein*], "In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the Internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic 'fingerprints' behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost."

> "Encryption" basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext". Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key".
>
> The applications of encryption, however, are not limited to ensuring secrecy; encryption can also be employed to ensure data integrity, authenticate users, and facilitate nonrepudiation ... It is, of course, encryption's secrecy applications that concern the government. The interception and deciphering of foreign communications has long played an important part of our nation's national security efforts.[179]

The government has expressed concern about enhancing individual privacy regarding internet usage and the deployment of successful encryption that prevents the state from intercepting communications. The result can be that the state is prevented from monitoring, investigating and prosecuting terrorists and other criminals who employ the internet for illegal purposes.[180] The debate surrounding the ability of law enforcement to intercept encrypted communications has been much more public than such a debate in Canada. In 1998, Robert S. Litt, Principal Associate Deputy Attorney General of the United States, testified:

> However, I don't think that it can reasonably be disputed that the unchecked spread of non-recoverable encryption will also endanger the public safety and our national security. People think of encryption primarily in the context of transmitted communications such as phone calls, and its effect on wiretaps. Indeed, it is absolutely essential that law enforcement preserve the ability to obtain plaintext of information from lawfully authorized wiretaps and authenticate this information in court. ... But if strong encryption becomes a standard feature, law enforcement will lose its ability to obtain and use this evidence. ... We believe that the most responsible solution is the development and widespread use of encryption systems, through a variety of technologies, permit timely access to plaintext by law enforcement authorities acting under lawful authority.[181]

While perhaps the issues surrounding encryption have not received as much public attention in Canada, law enforcement has undertaken

---

179 *Bernstein*, *ibid* at paras 17–18.

180 Hubbard "Wiretapping", *supra* note 9 at chapter 15.

181 Testimony of Robert S. Litt, Principal Associate Deputy Attorney General, before a subcommittee for the Senate on *Privacy in a Digital Age: Encryption and Mandatory Access* (presented March 17, 1998), online: <https://cryptome.org/jya/doj031798.htm>.

intense lobbying for unrestricted access to keys for encryption.[182] As early as 1998, Ontario's Privacy Commissioner, Dr. Ann Cavoukian, wrote about the tension between the public and private sides of the debate. She highlighted that the predicament faced by government is that requiring law enforcement to be provided with the key to decrypt encrypted communications almost completely undermines the point of cryptographic technology.[183] Once users of the technology are aware that others have the ability to decrypt their communications, they are likely to abandon the use of the technology because the protection offered to them has been eliminated.[184]

The difficulties continue when one looks at whether law enforcement should have access to the decryption key for 'in-transit' or archived communications. For archived communications, presumably law enforcement could obtain a production order requiring the service provider to produce the information, together with an assistance order requiring that the key to encryption be provided as well. For access to 'in-transit' communications, which is generally the goal of law enforcement's use of a Part VI Authorization, Dr. Cavoukian argues that several problems would arise:

> To be effective, access would have to be timely, a few hours after the transmission at the latest, and to achieve this quick turnaround time, the interception of the 'in-transit' encrypted message would have to be made before the content of the message was decrypted. A third party would have to hold the user's secret key since access through the user would alert the user. Then there is the issue of evidence. Until decrypted, the 'in-transit' message would have no evidentiary character, but the process of decryption would require court authorization.
> ...
> Indeed, the potential exists for lawful access to turn into massive 'fishing expeditions'. In this scenario, the balance between the interests of law enforcement, civil liberties and privacy would be struck largely in favour of law enforcement.[185]

---

182 Hubbard "Wiretapping", *supra* note 9 at chapter 15.

183 Ann Cavoukian, Submission to Industry Canada's Electronic Commerce Task Force *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*, (April 21, 1998) Information and Privacy Commissioner/Ontario 1 at 4, online: <https://www.ipc.on.ca/images/Resources/up-042198.pdf>).

184 *Ibid.*

185 *Ibid* at 6.

While the technical logistics and capabilities of communication encryption technology are beyond the scope of this paper when discussing the interception of in-transit communications, Part VI authorizations would be capable of including the interception and decryption of encrypted communications if legislation required service providers to retain decryption information. If law enforcement possessed a valid wiretap authorization that included an assistance order, requiring a service provider to retain decryption keys and provide those to law enforcement, then a wiretap authorization would be capable of covering encrypted messages. The true problem arises in that service providers are not required by legislation to retain such information and therefore do not have it to provide to law enforcement. As such, the ability of law enforcement to intercept some communications is thwarted, even when they are in possession of a wiretap authorization for which they have had to establish all of the statutory preconditions to the satisfaction of the issuing justice.

In 2005, the government introduced Bill C-74, the *Modernization of Investigative Techniques Act*,[186] which died on the order paper when the government was dissolved. The bill was based on two objectives: first, to compel telecommunication service providers to have the ability to intercept communications; and, second, to provide law enforcement with access to basic information identifying telecommunication service subscribers, upon request.[187] The proposed legislation was a culmination of an extensive consultation process in which over 300 submissions were received from police services, industry, civil rights groups, and individuals.[188] The proposed act would have required all telephone and internet providers to ensure that their infrastructures were intercept

---

186 *Bill C-74*, *Modernization of Investigative Techniques Act*, 1st sess, 38th Parl, 2005 (First Reading November 15, 2005) [*Bill C-74*]. A subsequent version of the Bill was introduced in 2007 as a Private Members' Bill however that too died on the order paper when Parliament was dissolved in the fall of 2008. No further legislation addressing this issue has been introduced.

187 *Ibid*.

188 Dominique Valiquet, "Telecommunications and Lawful Access: I. The Legislative Situation in Canada", (2006), Library of Parliament at p 3 [Valiquet, "Telecommunications].

capable.[189] Service providers would have been required to provide assistance to any law enforcement agency to permit it to access telecommunication facilities and provide a list of employees capable of providing such assistance.[190] Perhaps most importantly, the telecommunication service providers would have been required to give law enforcement access to decrypted communications and/or all reasonable assistance to decrypt it.[191] This would ensure that law enforcement, when in possession of a valid court order, is actually able to put that order into effect. The Canadian Association of Chiefs of Police continue to call for legislation that would compel telecommunication service providers to ensure their systems would be capable of allowing interception of communications.[192]

C. Access to Subscriber Information

Prior to the Supreme Court's decision of *R. v. Spencer*,[193] many viewed internet subscriber information as akin to the information one could find in a telephone book. When police were looking for a particular customer's name and address, the service provider would be contacted and, generally, the information would be given to police voluntarily and without the need for a warrant. That all changed with *Spencer*, with the court measuring what level of intimacy is connected to an individual's subscriber

---

189 *Bill C-74*, *supra* note 186 at cl 7(a). Clause 7(*a*) would have required that telecommunications service providers have the capability to intercept communications in accordance with the technical standards to be established in the regulations made under the proposed Act.

190 Valiquet, "Telecommunications" *supra* note 188. In addition, to being provided with a list of names of employees from the service providers, law enforcement would have been entitled to conduct a security assessment of the employees.

191 *Bill C-74*, *supra* note 186 at cl 6 (1)(b). If measures taken to protect a communication, such as encrypting or encoding, had been applied by someone other than the service provider and the service provider was unable to remove them, it would have then been required to provide all reasonable assistance to law enforcement agencies to do so (clauses 6(1)(*b*)(ii) and 6(2)).

192 Lawful Access Subcommittee, CACP Law Amendments Committee, "Lawful Access Reform: A Position Paper Prepared for the Canadian Association of Chiefs of Police" (2008), online: <https://www.cacp.ca/law-amendments-committee-activities.html?asst_id=437>.

193 2014 SCC 43, [2014] 2 SCR 212 [*Spencer*].

information and whether it falls into a category of information considered to be part of one's "biographical core" therefore protected by s. 8 of the *Charter*.[194]

The decision in *Spencer* had to examine the three digital s. 8 *Charter* doctrines that had developed over courts' decisions on technology: (1) the technological nature of the investigative technique; (2) the effect of contract and statute in shaping reasonable expectations of privacy; and (3) the application of the "biographical core" test to a category of information that some view as extremely intimate while others do not.[195]

The question of the effect of contract and statute was relatively easily set aside in that the court found that such considerations "may be relevant to, but not necessarily determinative of whether there is a reasonable expectation of privacy."[196]

The more interesting and thorough analysis came to the question of whether subscriber information is part of one's biographical core of information. It may be difficult to see how a customer's name, address and telephone number would reveal anything about a person's personal choices or details of one's lifestyle. However the court focused on what the name, address and telephone number actually gave the police. In this case, it gave them a connection to a computer they already knew to be downloading child pornography.

Two main arguments were presented in favour of demanding constitutional protection for subscriber information:

1. The information obtained by police (i.e. information likely to identify a person police know to be accessing child pornography) revealed "intimate details of the lifestyle and personal choices of the individual".[197] The fact that the details of the personal choices were illegal is immaterial because the activity is so intimate it deserves protection;
2. By obtaining an individual's subscriber information, police had the potential to observe online activity in a more sustained and general way.

---

194 *Ibid* at para 27.

195 Penney, "Digitization" *supra* note 126 at 507.

196 *Spencer*, *supra* note 193 at para 54.

197 *Ibid* at para 25.

Although the Court did not elaborate on how this could occur,[198] it was this second argument they endorsed in finding a reasonable expectation of privacy. They concluded that any request for subscriber information that corresponds to a "specifically observed, anonymous internet activity, engages a high level of informational privacy."[199]

The Court did not foreclose the possibility of a legislative response that would allow law enforcement to obtain such information without a warrant. In order to be compliant with s. 8 of the *Charter*, a search must be authorized by statute or at common law. The Court concluded that there was no authority for the search at common law and no statutory scheme, and therefore was left with the conclusion that the search was unreasonable.[200] Parliament could choose to regulate warrantless access to the information in a number of ways.

In Australia, legislation allows law enforcement agencies to access subscriber information without a warrant or court order.[201] The Australian approach established a database containing not only a subscriber's name, address and telephone number, but also the location of the device and whether it is used for government, business, charitable or private purposes.[202] Law enforcement agencies have access to this database for national security reasons, and for the purpose of enforcing criminal law. All telephone companies and re-sellers providing telephone and related services are required to provide information for the database on a daily basis.[203] Law enforcement agencies can access the database for national

---

198 Penney, "Digitization" *supra* note 126. Professor Penney notes that while it may be true that subscriber information could get police reams of personal information about internet usage, it is far from evident that that is correct. Commentators have also suggested that subscriber information gives police the potential to scour the internet for details records of someone's online activities, but there is no evidence in jurisprudence that this is something that the police have done, or even that law enforcement in Canada has the capability of doing this.

199 Spencer, *supra* note 193 at para 51.

200 Penney, "Digitization", *supra* note 126 at 533.

201 *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.

202 The Integrated Public Number Database, as established by the *Telecommunications Act 1997*, Part 4 of Schedule 2.

203 Robert W. Hubbard, Susan Magotiaux & Xenia Proestos, "The Limits of Privacy: Police Access to Subscriber Information in Canada" (2002) 46 Crim LQ 361 at 368.

security reasons and for enforcing criminal law and safeguarding public revenue in order to obtain the subscriber's name, address and telephone number, telephone's location where practicable, the name of the service provider providing the carriage service and whether the telephone is for government, private or personal use.[204]

In Canada, the proposed *Modernization of Investigative Techniques Act*[205] put forward that law enforcement have access to certain basic information identifying telecommunication service subscribers, without warrant or court order. The information to which law enforcement would have access would be limited to basic identifying information: name, IP address, email address, telephone numbers and any unique number associated to the device (i.e. presumably a cellular phone's IMEI[206] number). The telecommunication service providers would not have been required to collect information other than what they would have collected in the normal course of business, nor would they have been required to verify the accuracy of the customer information they were given.[207]

In the alternative of enacting legislation allowing for the warrantless access to subscriber information, Parliament could choose the addition of a specific warrant provision related to subscriber information. While police could currently apply for a search warrant under s. 487 of the *Criminal Code* for such information, they would be required to meet the threshold of *reasonable ground to believe* that there is anything that *will* afford evidence with respect to the commission of an offence in a particular place. This standard may be problematic for two reasons. First, police may not know which service provider is being used by a suspect therefore cannot specify an exact location where the evidence will be located. Second, requests for subscriber information are often made early

---

204 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, s 10.

205 *Bill C-74*, *supra* note 186.

206 IMEI is short for International Mobile Equipment Identity and is a unique number given to every mobile phone, typically found behind the battery. IMEI numbers of cellular phones connected to a Global System for Mobile Communications network are stored in a database containing all valid mobile phone equipment. When a phone is reported stolen or is not type approved, the number is marked invalid. (See Webopedia, online: <http://www.webopedia.com/TERM/I/IMEI.html> "IMEI").

207 *Bill C-74*, *supra* note 186.

in complex investigations, often to gather the information necessary to make an application for a wiretap authorization. At such an early stage of an investigation, it is unlikely that law enforcement would have sufficient information to meet the threshold of a s. 487 search warrant, namely reasonable grounds to believe.

Given the Supreme Court's recognition of a reasonable expectation of privacy in subscriber information, the enactment of legislation allowing a completely warrantless scheme for law enforcement's ability to receive subscriber information would be a lightening-rod for constitutional challenge. The most sensible approach for Parliament would be to introduce a form of production order unique to subscriber information, in direct response to the Supreme Court's decision in *Spencer*. While amendments to the *Criminal Code* in 2015 included a myriad of new warrants available to police in their investigations, the issue of subscriber data was not addressed. Allowing police to apply for an order on the standard of 'reasonable suspicion' would strike a balance between the privacy interests and reasonable expectation of privacy, as recognized by the Supreme Court, with the needs of law enforcement often early in an investigation.

VI. CONCLUSION

The way Canadians communicate with each other and around the world has evolved enormously since the 1970's. While speaking on a land-line telephone has not become completely obsolete, it has given way to conversations on cellular telephones, messages sent by text, and a huge variety of methods of communication over the internet. Canada's wiretap legislation has simply not kept up to the evolution of communication. This leaves law enforcement guessing at how the modern tools and techniques available to them fit with the existing legislation. It also leaves Canadian courts with the difficult task of attempting to fit modern tools and techniques into the confines of the near-ancient legislation, and historical concepts of an expectation of privacy that have emerged through the jurisprudence.

While some upgrading has occurred in the enactment of new legislative provisions often used in conjunction with a wiretap authorization, the attempts at modernization have not gone far enough. The core provisions of wiretap law must be updated to provide consistency

with the realities of modern wiretapping by law enforcement. Courts must also update their approach to the questions of admissibility of wiretap evidence to provide flexibility in historical concepts of an individual's reasonable expectation of privacy.

Both Parliament and the courts have a role to play. Amendments to legislation can be slow and tedious; however they provide the clearest definitions and parameters that, in turn, provide the greatest certainty and predictability to law enforcement attempting to properly investigate crime. Decisions of the courts can be reactionary to the facts of a particular case. However courts are able to consider the unique aspects of different modern tools and techniques available to law enforcement, therefore providing flexibility as new technology emerges. The goals and principles of practicality, flexibility, and consistency should govern the approaches taken by both Parliament and the courts in the constantly evolving considerations of wiretap law in Canada.