4 Private Communications

I. Introduction

One of the many blurred lines when it comes to applying *old* law to *new* technologies is the distinction between a seizure of historical communications and an intercept. The difference is significant. An intercept, colloquially called a wiretap, used to look very different from a seizure; clamps on wires allowed for listening in on conversations over phone lines or secret recorders captured voices in conversation. In 1975, Part VI of the *Criminal Code*[1] was added to completely govern the use and admissibility of wiretaps.

When conversations, and communications in general, take place through text, the application of the old regime is awkward. Now, wiretaps are largely wireless. A growing number of Canadians spend more time typing than talking on the phone. The *conversations* we have occur over wireless connections, and our words, voiceless, may travel in packets around and across the world before they are reconfigured in a recognizable form for the intended recipient. Even the *recipient* can be unclear: some communications are sent to a group or posted in a forum of anonymous usernames with a shifting and unknowable membership. The challenges for the criminal law in adapting Part VI to modern communications are many. As expressed by Moldaver J in *R v TELUS Communications Co*:

> 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.[2]

In order to determine whether a particular investigative technique is a gathering of data, a search or seizure, or an intercept under Part VI, courts must examine the definitions in Part VI and the objectives of that statutory package. Part VI defines *intercept* as "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof."[3] A private communication is defined as follows:

> "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.[4]

1 *Criminal Code*, RSC 1985, c C-46.

2 *R v TELUS Communications Co*, 2013 SCC 16, [2013] 2 SCR 3 at para 53 [*TELUS*].

3 *Criminal Code*, s 183.

4 *Ibid*.

Several problems arise in determining whether text communications are to be considered *private communications* for the purpose of Part VI. It is generally accepted that text-based communications can attract a reasonable expectation of privacy. A text message, on a secure network, that goes from one known person to another known person at a particular phone number, looks a lot like a voice conversation in terms of expected confidentiality.[5] However, depending on the nature of the communication and the circumstances of its making, there may be significant argument over whether it can reasonably be expected to be private. Several superior and appellate courts have found that particular online communications are not private communications.[6] What if the message goes to several recipients? Is an anonymous email the same as a text from one subscribed phone number to another? What if the recipients are unknown—usernames that have no connection to a name, location, or identity? As explored in Chapter 1, the reasonable expectation of privacy analysis is not an easy one in the digital context.

If the first hurdle is met and a communication is a private communication for the purposes of Part VI, it remains to be determined whether police acquisition of the communication is an intercept. That question was explored in depth, but not settled, in *TELUS*. In *TELUS*, the Supreme Court of Canada (SCC) issued three sets of reasons, each taking a different approach to the definition of intercept. The police had obtained general warrants pursuant to section 487.01 of the *Criminal Code* requiring a telecommunications company, Telus, to produce ongoing messages between two identified phone numbers. Importantly, the order was directed at communications that had not yet been made and was thus prospective in nature. The company was to provide police each day with the content of messages that had passed between those two numbers in the preceding 24 hours. The majority of the court found that prospective ongoing delivery of future communications required an authorization under Part VI. The path to that result was not consistent among judgments nor was it entirely clear.

The three sets of reason in *TELUS* were written by Abella J (with Fish J and LeBel J), Moldaver J (with Karakatsanis J) and Cromwell J (with McLachlin CJ). Abella J, writing for three justices, found that Part VI authorization (a wiretap) was required because an intercept occurs whenever the police acquire the content of a text message from a service provider who has stored it during the transmission process.[7]

Moldaver J agreed in the result—the future communications ordered to be delivered prospectively required a Part VI authorization. However, he declined to precisely define *intercept* and relied instead on a purposive consideration of the investigative

5 *TELUS*, *supra* note 2 at para 1; *R v Jones*, 2016 ONCA 543 at para 25.

6 See e.g. *R v Allen*, 2017 ONSC 1712; *R v Mills*, 2017 NLCA 12; *R v Ghotra*, [2015] OJ No 7253 (Sup Ct J); and *R v Graff*, 2015 ABQB 415, where online communications were found not to be private communications.

7 *Supra* note 2 at paras 1-46.

proposal. He found that courts should approach the question from a standpoint of substantial equivalence—that is, if what the police are seeking in substance looks like an intercept, then that is the appropriate form and standard of pre-authorization.[8]

The third set of *TELUS* reasons differed in the result and raised flags about the implications of Abella J's decision. McLachlin CJ and Cromwell J dissented, and commented that the definition of intercept proposed by Abella J would undermine well-established law that said stored communications, already delivered, were accessible by search warrant.[9] Text communications may have been intercepted by Telus, but police did not *intercept* them when they obtained the already stored messages. The dissenters would have found that the general warrant, not an authorization for interception, could properly support the police request.

The ultimate holding in *TELUS* was strictly limited: police require Part VI authorization when they are seeking a prospective order for future communications. Outside of that narrow ratio, more questions are raised than answered in the judgments.

II. Historical Stored Communications

The issue of historical communications has been plaguing courts somewhat since *TELUS*, and will be returning to the top court for direct consideration in *Jones*.[10]

Historically, police obtained stored prior communications via a search warrant to access a computer or a production order served on a telecommunications company that stored text-based messages for some period after delivery. An email that was sent, read, and stored on a recipient's computer could be reviewed by police under a warrant obtained for the seizure of the computer. Lawful analysis of the device could include examination of any files on the computer, including sent and received emails stored therein. Interception was understood as an act intervening between the sending and the receipt.

In *TELUS*, Abella J wrote that contemporaneity was not an element of the definition of intercept. That is, communications do not have to be caught in transit to be intercepted. Because the definition of intercept refers to the acquisition of meaning of a communication, a plain reading of the text could result in finding that anytime police listen to or acquire the meaning of a private communication, they are engaging in an intercept. Taken to the extreme, that could mean that when police seize a computer under a search warrant and examine stored emails from years before, they are

8 *Ibid* at paras 47-108. Moldaver J was influenced by the statutory exclusion of the use of general warrants where another authorization was available in the *Criminal Code* (s 487.01(1)(c)) and by the fact that the statutory preconditions for an intercept were significantly more onerous than the general warrant.

9 *Ibid* at paras 109-196; see reference to the inconsistency between the reasons of Abella J and prior law on computer searches of stored communications at para 155.

10 *Jones*, *supra* note 5, leave to appeal to SCC granted, 37194 (17 November, 2016).

in fact intercepting those communications, although note that Abella J also required that the communications be acquired by the police in the course of the communications process.[11] In the dissent, Cromwell J argued that such an interpretation would run counter to years of search law, up to the SCC itself, where stored historical messages were reviewed and relied on when obtained through traditional warrants that were not Part VI authorizations.[12]

Courts across Canada have varied in their application of *TELUS*; however, most courts have held that Part VI does not apply to stored historical communications. In *R v Belcourt*, a unanimous British Columbia Court of Appeal found that Part VI was limited to prospective evidence gathering.[13] The court in *Belcourt* reviewed *TELUS* in detail and further considered the purpose and ambit of Part VI in comparison with traditional search warrants. The court concluded that the retrospective nature of historical stored texts excluded them from Part VI consideration:

> As I have said, the acquisition of stored, historical communications is not, and cannot be, prospective. As a result, it is outside the ambit of Part VI of the *Code* to require that existing communications stored in electronic form be authorized under that section. In my view, requiring Part VI authorization for acquisitions of evidence already in existence is inconsistent with the law of search and seizure in Canada.[14]

The Court of Appeal for Ontario similarly concluded that there is a temporal aspect to Part VI—communications already in existence are not covered. In *Jones*, the majority of the court found:

> To fall under Part VI, there needs to be a prospective component to the private communications, otherwise the communications are not being intercepted. This is because the word "intercept" suggests an interference between the place of origin and the destination of the private communication. There is no such interference when obtaining historical text messages stored on a phone or a service provider's server.[15]

And later:

> I would not describe the production of historical text messages as surveillance or an interception. It is, quite simply, a search and seizure of a historical record of text messages sent and received in the past.[16]

11 *TELUS*, *supra* note 2 at para 37.

12 *Ibid* at para 155, Cromwell J, dissenting. See also *Jones*, *supra* note 5 at para 35.

13 *R v Belcourt*, 2015 BCCA 126.

14 *Ibid* at para 50.

15 *Jones*, *supra* note 5 at para 30.

16 *Ibid* at para 31. See also *R v Nero*, 2016 ONCA 160.

The court in *Jones* also cited their own additional post-*TELUS* jurisprudence supporting the prospective nature of the wiretap provisions. Both *Nero* and *R v Beauchamp* found that wiretap authorizations related to communications that had not yet taken place and indeed may never occur.[17] Other cases have reached the contrary result and applied Part VI authorizations to stored communications in the possession of telecommunications providers.[18]

A trickier distinction arises when police obtain a copy of a communication that has been sent and not yet received. The temporal connection to the concept of intercept that grounded the decisions in *Belcourt* and *Jones* does not provide a clear-cut answer to the situation of a past communication that has not yet been, and perhaps never will be, received. Technologically, *receipt* may be difficult to define.[19] For example, if an email is sent to a web-based email address, and the intended recipient never accesses that message despite the fact that it's sitting in a virtual inbox, will any future capture of that message be considered an intercept? Defence counsel will challenge the capture of a message not yet read as an intercept, a stepping between two parties to a communication. The state will counter that the message has indeed been received at its destination regardless of what attention has been paid, and, like a recorded voice mail, reviewing its contents will not require Part VI authorization. The historical and the prospective may be hard to separate with digital communications.

One scenario in which this problem will often arise is where the police seize the accused's device upon arrest, and then search the text communications stored on the device—either pursuant to judicial authorization or the search incident to arrest power. When the device was not turned off or put on "airplane mode" immediately upon arrest, the device will have continued to receive emails and text messages even after it came into police possession. Indeed, some of these emails and text messages could even have come from the accused's lawyer. Defence counsel should therefore be careful about communicating with their clients through text communications when their devices have been seized, particularly given their duty to take "all reasonable steps to ensure the privacy and safekeeping of a client's confidential information."[20]

III. One-Party Consent

When Part VI of the *Criminal Code* was enacted, it covered traditional third-party wiretaps: intercepts where the parties being *listened to* when unaware of the recording of the communications. After the SCC case of *Duarte*,[21] the *Criminal Code* was amended to provide for judicial authorization of one-party consent intercepts: those where the police (or an agent or cooperating person) engage in and record

17 *R v Beauchamp*, 2015 ONCA 260; *Nero*, *supra* note 16.

18 *R v Croft*, [2013] AJ No 1231 (QB); *R v Hoelscher*, 2016 ABQB 44.

19 *TELUS*, *supra* note 2 at para 34, Abella J; *Belcourt*, *supra* note 13 at paras 45-46.

20 Law Society of Upper Canada, *Rules of Professional Conduct*, LSUC, Toronto: 2000, as amended, r 3.5-2, commentary [2], r 3.3-1.

21 *R v Duarte*, [1990] 1 SCR 30.

communications with an unknowing target. One party to the communication is aware of and consenting to the intercept. Interception where one person is consenting is not a criminal offence. It may, however, be unconstitutional where the consenter is a state actor. Again, the boundaries of the law are unclear in the context of digital communications.

The key case in the area of one-party consent intercepts is *Duarte*. In *Duarte*, the SCC held that surreptitious electronic recording of verbal discussions between a target and an undercover officer, without prior judicial authorization, constituted an unreasonable search and seizure and infringed section 8 of the Charter.[22] The court held that an officer's creation of a permanent electronic record presented a risk to a person's privacy of "a different order of magnitude" than an officer's memory of a conversation.

In 1990, when *Duarte* was decided on the issue of recording communications, La Forest J, writing for the majority, was concerned with the state taking the transient spoken word and immortalizing it in exact replica. He wrote that privacy would be destroyed if the state were free to make surreptitious permanent electronic recordings of our private communications.[23] Pre-authorization was required to guard against the "insidious danger" that the state would "record and transmit our words."[24]

We have come a significant distance since the secret capturing of fleeting verbal utterances in *Duarte*. Unlike the voices in *Duarte*, text-based communications are not transformed by the state. The majority of the Court of Appeal in Ontario noted that "[t]he key point in *Duarte* was that the state surreptitiously created a permanent record of oral conversations, where otherwise none would exist."[25] When the sender is the one who creates the permanent record, in the very form and medium that police ultimately wish to use as evidence, is the act of the state a violation? What if the police have to take certain additional steps in order to create a record of the conversation, even if it's as simple as checking off a box to save all of the Internet chatroom conversations? Does that change the analysis?

The circumstances in which a conversation is taking place are also relevant. Sometimes, the sender of a text communication does not see and may not know the recipient beyond the listing of a made-up username. The sender cannot know or control whether the recipient will share, store, print, copy, or destroy the electronic record that is transmitted; although, again, the defence will argue against the *assumption of risk doctrine* playing a role in the section 8 analysis.[26]

22 *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.

23 *Duarte*, *supra* note 21 at 44.

24 *Ibid* at 43-44.

25 *R v Marakah*, 2016 ONCA 542 at para 82.

26 *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 at para 76; *Duarte*, *supra* note 21 at 47-48; *R v Wong*, [1990] 3 SCR 36 at 45.

The arguments about *Duarte*'s application to online communications have not been directly considered by the SCC. Like the issue of stored historical communications, prior discussion of section 8 in online communications has appeared to accept, without argument, that no authorization to intercept is required. For example, in the case of *R v Levigne*, the SCC considered an online luring case that involved police engaging in undercover digital communications with the accused, Mr. Levigne, who thought he was communicating with a child.[27] Police officers had no Part VI authorization. They were engaged in online undercover communications, which were admitted at trial. The SCC considered arguments about the parameters of the offence of luring, but no one raised the possibility that an authorization to intercept ought to have been obtained to permit the storage and admission of the online chats by the state actors.

The Newfoundland and Labrador Court of Appeal endorsed the conclusion that online undercover chats do not require a Part VI authorization (a consent wire).[28] In *Mills*, an officer created a Hotmail account and Facebook profile for a fictitious teenager. Mr. Mills made a friend request and starting communicating with the fictitious teen by email. He claimed he was a 23-year-old male, though he was in fact nine years older. The officer kept records of the emails through a program called Snagit. The court found unanimously that the online undercover communications by the officer did not constitute an interception and no Part VI authorization was required.

The Superior Court of Ontario reached a similar decision in *Ghotra*[29] after thorough analysis of *Duarte* and the nature of online communications. Durno J emphasized that the individual, not the state, created a permanent electronic record and relinquished it in a forum where he could have only a hope that the recipient would treat it as private. Although he accepted that the accused may have had a subjective expectation of privacy, he found that such an expectation could not be objectively reasonable. Durno J gave four key factors for his conclusion that no reasonable expectation of privacy arose in this context:

> First, while the Supreme Court of Canada held in *TELUS* that text messages are "made under circumstances that attract a reasonable expectation of privacy …" at para. 32, I am persuaded that not every text message in every context attracts a reasonable expectation of privacy. The Court's comments are a valuable starting point. However, the context in which the communication takes place including with who the participants think they are communicating is important.
>
> Second, while *Duarte* addresses the concerns for the state surreptitiously creating a record of a communication that does not generate its own record, those concerns do not apply to text messages. This case does not involve oral communication and the state

27 *R v Levigne*, 2010 SCC 25, [2010] 2 SCR 3.

28 *Mills*, *supra* note 6.

29 *Ghotra*, *supra* note 6.

creating the record. By their nature text messages create a record of the communications. They already exist and the participants know there is a record. They create it, see it and can access it on their computers.

Third, that the applicant went from a public chat room to one where it was reasonable to conclude would be a private discussion between two people is a factor to consider. However, in itself it is not determinative as it can be seen as simply reducing the number of persons who know what is being discussed. The applicant went from a public chat room where he had no idea who he was communicating with to a private chat with a total stranger. The label "private chat room" is not determinative. If there is no reasonable expectation of privacy in the conversation, where it occurred is not determinative. A private chat means one that is not seen or heard by others in the chat room. It does not mean it cannot be recorded and saved.

Fourth, I find it is relevant that the chat was with a stranger. I am not persuaded that that fact is irrelevant nor do I accept the applicant's argument that any drug deal conversations between buyers and sellers always involve strangers. Often the communications are between persons who have had drug dealings in the past and result in multiple purchases before arrests are made.[30]

With regard to the loss of control over text communications, and the risk that the recipients can do what they will with the recordings, Durno J concluded:

> The parties are communicating over a medium that requires written, not verbal communications. It is apparent that role-playing and deception are common on the internet. The applicant told Mia that his first name was Annan. His first name is Akash. There is no history between the persons. Nothing was texted that suggested concerns for privacy. It is unrealistic to suggest that there is some sort of presumption that a stranger would comply with the applicant's or anyone else's views of privacy. A party to a text conversation with someone he or she does not know might have a hope that whomever he or she is communicating with will respect their privacy. Hoping and having a reasonable expectation are not synonymous in this context. Once the applicant typed the messages, he lost all control over their use.[31]

The analysis and conclusion in *Ghotra* were echoed in *R v Allen*, another luring case in the Ontario Superior Court of Justice.[32] Again, the court found no reasonable expectation of privacy in the chats and determined that there was no *intercept*, so Part VI was not engaged.[33] The court reached a different conclusion in *R v Kwok*. There, the court found that the accused's online conversation with the undercover in a private chat room were "private communications" within the meaning of Part VI. Also,

30 *Ibid* at paras 124-27.

31 *Ibid* at para 129.

32 *Allen*, *supra* note 6.

33 *Ibid* at para 73.

because the officer had the option of disabling the function to keep a record of the conversations but did not do so, the court held that the officer intercepted those communications and should have obtained judicial authorization before doing so.[34] Of course, this is just a provincial court decision. There does not appear to be any higher authority on this side of the debate. The issue of whether and how Part VI applies to online chats remains unresolved.

It cannot be said categorically that all online communications will or will not be found to be *private communications* for the purposes of Part VI of the *Criminal Code*. Counsel may need to create a thorough record of the nature of the communications, the nature of any relationship between the sender and recipient, the online setting and its disclaimers or access controls, and any privacy requests or assurances directly made in communications. All of these factors can be weighed by the court to determine whether there is a reasonable expectation of privacy in the totality of circumstances. Parties should not take for granted that a court will have the technical knowledge or understanding to properly determine boundaries of privacy without evidence.

IV. Summary

The interception of private communications is a topic bound to experience significant upheaval in the near future. Part VI of the *Criminal Code*, and the common law, mainly *Duarte*, were written at a time when wiretapping meant surreptitiously transforming ethereal voices into permanent electronic records. Electronic (digital) records are now the starting point, not the secret end, of modern communications. We need to adapt.

As counsel navigate the boundaries between search and intercept, there will be a need to educate both themselves and the court in order to ensure a proper understanding of the technique used or contemplated and the scope of privacy interests potentially engaged. For Crown counsel and police, well-trained and specialized officers are extremely valuable in the early stages of explaining to issuing justices and courts the nature of technologies used and evidence produced. Of course, specialized units are not available in all areas of the country or in all police services. Defence counsel can push for disclosure of tools and techniques and ensure that they are themselves knowledgeable enough to test police evidence about the nature of digital communications. It may also be essential to retain a forensic expert to ensure that defence counsel are asking the right questions.

34 *R v Kwok*, [2008] OJ No 2414 at para 22 (Ont CJ).

APPENDIX 4.1

Criminal Code

RSC 1985, c C-46 , ss 183-186.1

Part VI Invasion of Privacy

Definitions

183 In this Part,

. . .

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;

. . .

"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.

. . .

Interception of Communications

Interception

184(1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Saving provision

(2) Subsection (1) does not apply to

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service;

(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or

(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for

(i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or

(ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).

Use or retention

(3) A private communication intercepted by a person referred to in paragraph (2)(e) can be used or retained only if

(a) it is essential to identify, isolate or prevent harm to the computer system; or

(b) it is to be disclosed in circumstances referred to in subsection 193(2).

Interception to prevent bodily harm

184.1(1) An agent of the state may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if

(a) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception;

(b) the agent of the state believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception; and

(c) the purpose of the interception is to prevent the bodily harm.

Admissibility of intercepted communication

(2) The contents of a private communication that is obtained from an interception pursuant to subsection (1) are inadmissible as evidence except for the purposes of proceedings in which actual, attempted or threatened bodily harm is alleged, including proceedings in respect of an application for an authorization under this Part or in respect of a search warrant or a warrant for the arrest of any person.

Destruction of recordings and transcripts

(3) The agent of the state who intercepts a private communication pursuant to subsection (1) shall, as soon as is practicable in the circumstances, destroy any recording of the private communication that is obtained from an interception pursuant to subsection (1), any full or partial transcript of the recording and any notes made by that agent of the private communication if nothing in the private communication

suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur.

Definition of *agent of the state*

(4) For the purposes of this section, *agent of the state* means

(a) a peace officer; and

(b) a person acting under the authority of, or in cooperation with, a peace officer.

Interception with consent

184.2(1) A person may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where either the originator of the private communication or the person intended by the originator to receive it has consented to the interception and an authorization has been obtained pursuant to subsection (3).

Application for authorization

(2) An application for an authorization under this section shall be made by a peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, *ex parte* and in writing to a provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552, and shall be accompanied by an affidavit, which may be sworn on the information and belief of that peace officer or public officer or of any other peace officer or public officer, deposing to the following matters:

(a) that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed;

(b) the particulars of the offence;

(c) the name of the person who has consented to the interception;

(d) the period for which the authorization is requested; and

(e) in the case of an application for an authorization where an authorization has previously been granted under this section or section 186, the particulars of the authorization.

Judge to be satisfied

(3) An authorization may be given under this section if the judge to whom the application is made is satisfied that

(a) there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed;

(b) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and

(c) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought.

Content and limitation of authorization

(4) An authorization given under this section shall

(a) state the offence in respect of which private communications may be intercepted;

(b) state the type of private communication that may be intercepted;

(c) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given, and generally describe the manner of interception that may be used;

(d) contain the terms and conditions that the judge considers advisable in the public interest; and

(e) be valid for the period, not exceeding sixty days, set out therein.

Related warrant or order

(5) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018, 487.02, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order is related to the execution of the authorization.

Application by means of telecommunication

184.3(1) Notwithstanding section 184.2, an application for an authorization under subsection 184.2(2) may be made *ex parte* to a provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552, by telephone or other means of telecommunication, if it would be impracticable in the circumstances for the applicant to appear personally before a judge.

Application

(2) An application for an authorization made under this section shall be on oath and shall be accompanied by a statement that includes the matters referred to in paragraphs 184.2(2)(a) to (e) and that states the circumstances that make it impracticable for the applicant to appear personally before a judge.

Recording

(3) The judge shall record, in writing or otherwise, the application for an authorization made under this section and, on determination of the application, shall cause the writing or recording to be placed in the packet referred to in subsection 187(1) and sealed in that packet, and a recording sealed in a packet shall be treated as if it were a document for the purposes of section 187.

Oath

(4) For the purposes of subsection (2), an oath may be administered by telephone or other means of telecommunication.

Alternative to oath

(5) An applicant who uses a means of telecommunication that produces a writing may, instead of swearing an oath for the purposes of subsection (2), make a statement in writing stating that all matters contained in the application are true to the knowledge or belief of the applicant and such a statement shall be deemed to be a statement made under oath.

Authorization

(6) Where the judge to whom an application is made under this section is satisfied that the circumstances referred to in paragraphs 184.2(3)(a) to (c) exist and that the circumstances referred to in subsection (2) make it impracticable for the applicant to appear personally before a judge, the judge may, on such terms and conditions, if any, as are considered advisable, give an authorization by telephone or other means of telecommunication for a period of up to thirty-six hours.

Giving authorization

(7) Where a judge gives an authorization by telephone or other means of telecommunication, other than a means of telecommunication that produces a writing,

(a) the judge shall complete and sign the authorization in writing, noting on its face the time, date and place at which it is given;

(b) the applicant shall, on the direction of the judge, complete a facsimile of the authorization in writing, noting on its face the name of the judge who gave it and the time, date and place at which it was given; and

(c) the judge shall, as soon as is practicable after the authorization has been given, cause the authorization to be placed in the packet referred to in subsection 187(1) and sealed in that packet.

Giving authorization where telecommunication produces writing

(8) Where a judge gives an authorization by a means of telecommunication that produces a writing, the judge shall

(a) complete and sign the authorization in writing, noting on its face the time, date and place at which it is given;

(b) transmit the authorization by the means of telecommunication to the applicant, and the copy received by the applicant shall be deemed to be a facsimile referred to in paragraph (7)(b); and

(c) as soon as is practicable after the authorization has been given, cause the authorization to be placed in the packet referred to in subsection 187(1) and sealed in that packet.

Immediate interception—imminent harm

184.4 A police officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if the police officer has reasonable grounds to believe that

(a) the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;

(b) the interception is immediately necessary to prevent an offence that would cause serious harm to any person or to property; and

(c) either the originator of the private communication or the person intended by the originator to receive it is the person who would commit the offence that is likely to cause the harm or is the victim, or intended victim, of the harm.

Interception of radio-based telephone communications

184.5(1) Every person who intercepts, by means of any electro-magnetic, acoustic, mechanical or other device, maliciously or for gain, a radio-based telephone communication, if the originator of the communication or the person intended by the originator of the communication to receive it is in Canada, is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Other provisions to apply

(2) Section 183.1, subsection 184(2) and sections 184.1 to 190 and 194 to 196 apply, with such modifications as the circumstances require, to interceptions of radio-based telephone communications referred to in subsection (1).

One application for authorization sufficient

184.6 For greater certainty, an application for an authorization under this Part may be made with respect to both private communications and radio-based telephone communications at the same time.

Application for authorization

185(1) An application for an authorization to be given under section 186 shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 and shall be signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness or an agent specially designated in writing for the purposes of this section by

(a) the Minister personally or the Deputy Minister of Public Safety and Emergency Preparedness personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or

(b) the Attorney General of a province personally or the Deputy Attorney General of a province personally, in any other case,

and shall be accompanied by an affidavit, which may be sworn on the information and belief of a peace officer or public officer deposing to the following matters:

(c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence,

(d) the type of private communication proposed to be intercepted,

(e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,

(f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made,

(g) the period for which the authorization is requested, and

(h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

Exception for criminal organizations and terrorist groups

(1.1) Notwithstanding paragraph (1)(h), that paragraph does not apply where the application for an authorization is in relation to

(a) an offence under section 467.11, 467.111, 467.12 or 467.13;

(b) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(c) a terrorism offence.

Extension of period for notification

(2) An application for an authorization may be accompanied by an application, personally signed by the Attorney General of the province in which the application for the authorization is made or the Minister of Public Safety and Emergency Preparedness if the application for the authorization is made by him or on his behalf, to substitute for the period mentioned in subsection 196(1) such longer period not exceeding three years as is set out in the application.

Where extension to be granted

(3) Where an application for an authorization is accompanied by an application referred to in subsection (2), the judge to whom the applications are made shall first consider the application referred to in subsection (2) and where, on the basis of the affidavit in support of the application for the authorization and any other affidavit evidence submitted in support of the application referred to in subsection (2), the judge is of the opinion that the interests of justice warrant the granting of the application, he shall fix a period, not exceeding three years, in substitution for the period mentioned in subsection 196(1).

Where extension not granted

(4) Where the judge to whom an application for an authorization and an application referred to in subsection (2) are made refuses to fix a period in substitution for the period mentioned in subsection 196(1) or where the judge fixes a period in substitution therefor that is less than the period set out in the application referred to in subsection (2), the person appearing before the judge on the application for the authorization may withdraw the application for the authorization and thereupon the judge shall not proceed to consider the application for the authorization or to give the authorization and shall return to the person appearing before him on the application for the authorization both applications and all other material pertaining thereto.

Judge to be satisfied

186(1) An authorization under this section may be given if the judge to whom the application is made is satisfied

(a) that it would be in the best interests of the administration of justice to do so; and

(b) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

Exception for criminal organizations and terrorism offences

(1.1) Notwithstanding paragraph (1)(b), that paragraph does not apply where the judge is satisfied that the application for an authorization is in relation to

(a) an offence under section 467.11, 467.111, 467.12 or 467.13;

(b) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(c) a terrorism offence.

Where authorization not to be given

(2) No authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom

the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other such solicitor or a member of the solicitor's household has been or is about to become a party to an offence.

Terms and conditions

(3) Where an authorization is given in relation to the interception of private communications at a place described in subsection (2), the judge by whom the authorization is given shall include therein such terms and conditions as he considers advisable to protect privileged communications between solicitors and clients.

Content and limitation of authorization

(4) An authorization shall

(a) state the offence in respect of which private communications may be intercepted;

(b) state the type of private communication that may be intercepted;

(c) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given, and generally describe the manner of interception that may be used;

(d) contain such terms and conditions as the judge considers advisable in the public interest; and

(e) be valid for the period, not exceeding sixty days, set out therein.

Persons designated

(5) The Minister of Public Safety and Emergency Preparedness or the Attorney General, as the case may be, may designate a person or persons who may intercept private communications under authorizations.

Installation and removal of device

(5.1) For greater certainty, an authorization that permits interception by means of an electro-magnetic, acoustic, mechanical or other device includes the authority to install, maintain or remove the device covertly.

Removal after expiry of authorization

(5.2) On an *ex parte* application, in writing, supported by affidavit, the judge who gave an authorization referred to in subsection (5.1) or any other judge having jurisdiction to give such an authorization may give a further authorization for the covert removal of the electro-magnetic, acoustic, mechanical or other device after the expiry of the original authorization

(a) under any terms or conditions that the judge considers advisable in the public interest; and

(b) during any specified period of not more than sixty days.

Renewal of authorization

(6) Renewals of an authorization may be given by a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 on receipt by him or her of an *ex parte* application in writing signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness—or an agent specially designated in writing for the purposes of section 185 by the Minister or the Attorney General, as the case may be—accompanied by an affidavit of a peace officer or public officer deposing to the following matters:

(a) the reason and period for which the renewal is required,

(b) full particulars, together with times and dates, when interceptions, if any, were made or attempted under the authorization, and any information that has been obtained by any interception, and

(c) the number of instances, if any, on which, to the knowledge and belief of the deponent, an application has been made under this subsection in relation to the same authorization and on which the application was withdrawn or no renewal was given, the date on which each application was made and the name of the judge to whom each application was made,

and supported by such other information as the judge may require.

Renewal

(7) A renewal of an authorization may be given if the judge to whom the application is made is satisfied that any of the circumstances described in subsection (1) still obtain, but no renewal shall be for a period exceeding sixty days.

Related warrant or order

(8) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018, 487.02, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order is related to the execution of the authorization.

Time limitation in relation to criminal organizations and terrorism offences

186.1 Notwithstanding paragraphs 184.2(4)(e) and 186(4)(e) and subsection 186(7), an authorization or any renewal of an authorization may be valid for one or more periods specified in the authorization exceeding sixty days, each not exceeding one year, where the authorization is in relation to

(a) an offence under section 467.11, 467.111, 467.12 or 467.13;

(b) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(c) a terrorism offence.