SUPREME COURT OF CANADA

CITATION: R. *v.* TELUS Communications Co., 2013 SCC 16

DATE: 20130327
DOCKET: 34252

BETWEEN:

TELUS Communications Company
Appellant
and
Her Majesty The Queen
Respondent
- and -
Attorney General of Ontario, Canadian Civil Liberties Association and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
Interveners

CORAM: McLachlin C.J. and LeBel, Fish, Abella, Cromwell, Moldaver and Karakatsanis JJ.

REASONS FOR JUDGMENT: Abella J. (LeBel and Fish JJ. concurring)
(paras. 1 to 46)

REASONS CONCURRING IN PART AND IN RESULT: Moldaver J. (Karakatsanis J. concurring)
(paras. 47 to 108)

DISSENTING REASONS: Cromwell J. (McLachlin C.J. concurring)
(paras. 109 to 196)

TELUS Communications Company *Appellant*

v.

Her Majesty The Queen *Respondent*

and

Attorney General of Ontario, Canadian Civil Liberties Association and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic *Interveners*

Indexed as: R. *v.* TELUS Communications Co.

2013 SCC 16

File No.: 34252.

2012: October 15; 2013: March 27.

Present: McLachlin C.J. and LeBel, Fish, Abella, Cromwell, Moldaver and Karakatsanis JJ.

ON APPEAL FROM THE ONTARIO SUPERIOR COURT OF JUSTICE

Criminal law — Interception of communications — General warrant — Telecommunications company employing unique process for transmitting text messages resulting in messages stored on their computer database for brief period of time — General warrant requiring telecommunications company to produce all text messages sent and received by two subscribers on prospective, daily basis — Whether general warrant power in s. 487.01 of Criminal Code can authorize prospective production of future text messages from service provider's computer — Whether investigative technique authorized by general warrant in this case is an interception requiring authorization under Part VI of Criminal Code — Whether general warrant may properly issue where substance of investigative technique, if not its precise form, is addressed by existing legislative provision — Criminal Code, R.S.C. 1985, c. C-46, ss. 487.01.

Unlike most telecommunications service providers, TELUS Communications Company routinely makes electronic copies of all the text messages sent or received by its subscribers and stores them on a computer database for a brief period of time. The police in this case obtained a general warrant and related assistance order under ss. 487.01 and 487.02 of the *Criminal Code* requiring Telus to provide the police with copies of any stored text messages sent or received by two Telus subscribers. The relevant part of the warrant required Telus to produce any messages sent or received during a two-week period on a daily basis. Telus applied to quash the general warrant arguing that the prospective, daily acquisition of text messages from their computer database constitutes an interception of private

communications and therefore requires authorization under the wiretap authorization provisions in Part VI of the *Code*. The application was dismissed. The focus of the appeal is on whether the general warrant power can authorize the prospective production of future text messages from a service provider's computer.

Held (McLachlin C.J. and Cromwell J. dissenting): The appeal should be allowed and the general warrant and related assistance order should be quashed.

Per LeBel, Fish and **Abella** JJ.: Part VI of the *Criminal Code* provides a comprehensive scheme for "wiretap authorizations" for the interception of private communications. The purpose of Part VI is to restrict the ability of the police to obtain and disclose private communications.

Telus employs a unique process for transmitting text messages that results in the messages being stored on their computer database for a brief period of time. In considering whether the prospective, daily production of future text messages stored in Telus' computer falls within Part VI, we must take the overall objective of Part VI into account.

Text messaging is, in essence, an electronic conversation. Technical differences inherent in new technology should not determine the scope of protection afforded to private communications. The only practical difference between text messaging and traditional voice communications is the transmission process. This

distinction should not take text messages outside the protection to which private communications are entitled under Part VI.

Section 487.01 of the *Code*, the general warrant provision, was enacted in 1993 as part of a series of amendments to the *Code* in Bill C-109, S.C. 1993, c. 40. It authorizes a judge to issue a general warrant permitting a peace officer to "use any device or investigative technique or procedure or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure". Notably, s. 487.01(1)(*c*) stipulates that the general warrant power is residual and resort to it is precluded where judicial approval for the proposed technique, procedure or device or the "doing of the thing" is available under the *Code* or another federal statute.

Section 487.01(1)(*c*) should be broadly construed to ensure that the general warrant is not used presumptively to prevent the circumvention of the more specific or rigorous pre-authorization requirements for warrants, such as those found in Part VI. To decide whether s. 487.01(1)(*c*) applies, namely, whether another provision would provide for the authorization sought in this case, requires interpreting the word "intercept" in Part VI. "Intercept" is used throughout Part VI with reference to the intercept *of private communications*. This means that in interpreting "intercept a private communication", we must consider the broad scope of Part VI and its application across a number of technological platforms, as well as its objective of protecting individual privacy interests in communications by imposing particularly rigorous safeguards. The interpretation should not be dictated by the technology used

to transmit such communications, like the computer used in this case, but by what was intended to be protected under Part VI. It should also be informed by the rights enshrined in s. 8 of the *Charter*, which in turn must remain aligned with technological developments.

A technical approach to "intercept" would essentially render Part VI irrelevant to the protection of the right to privacy in new, electronic and text-based communications technologies, which generate and store copies of private communications as part of the transmission process. A narrow definition is also inconsistent with the language and purpose of Part VI in offering broad protection for private communications from unauthorized interference by the state.

The interpretation of "intercept a private communication" must, therefore, focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made. To the extent that there may be any temporal element inherent in the technical meaning of intercept, it should not trump Parliament's intention in Part VI to protect an individual's right to privacy in his or her communications. The use of the word "intercept" implies that the private communication is acquired in the course of the communication process. The process encompasses all activities of the service provider which are required for, or incidental to, the provision of the communications service. Acquiring the substance of a private communication from a computer maintained by a telecommunications service provider would, as a result, be included in that process.

Text messages are private communications and, even if they are stored on a service provider's computer, their prospective production requires authorization under Part VI of the *Code*. If Telus did not maintain its computer database, there is no doubt that the police would be required to obtain an authorization under Part VI to secure the prospective, and in this case continuous, production of text messages. Most service providers do not routinely copy text messages to a computer database as part of their transmission service. Accordingly, if the police wanted to target an individual who used a different service provider, they would have no option but to obtain wiretap authorizations under Part VI to compel the prospective and continuous production of their text messages. This creates a manifest unfairness to individuals who are unlikely to realize that their choice of telecommunications service provider can dramatically affect their privacy. The technical differences inherent in Telus' transmission of text messages should not deprive Telus subscribers of the protection of the *Code* that every other Canadian is entitled to.

The general warrant in this case was invalid because the police had failed to satisfy the requirement under s. 487.01(1)(*c*) of the *Code* that a general warrant could not be issued if another provision in the *Code* is available to authorize the technique used by police. Since the warrant purports to authorize the interception of private communications, and since Part VI is the scheme that authorizes the interception of private communications, a general warrant was not available.

Per **Moldaver** and Karakatsanis JJ.: There is agreement with Abella J. that the police are entitled to a general warrant only where they can show that "no other provision" of the *Criminal Code* or any other Act of Parliament would provide for the investigative technique, including a substantively equivalent technique, for which authorization is sought. The investigative technique in this case was substantively equivalent to an intercept. The general warrant is thus invalid. Resolution of whether what occurred in this case was or was not, strictly speaking, an "intercept" within the meaning of s. 183 of the *Code* is unnecessary. A narrower decision guards against unforeseen and potentially far-reaching consequences in this complex area of the law.

The result is driven by the failure of the authorities to establish the requirement in s. 487.01(1)(*c*) that there be "no other provision" that would provide for the search. This provision ensures that the general warrant is used sparingly as a warrant of limited resort. In creating the general warrant, Parliament did not erase every other search authorization from the *Code* and leave it to judges to devise general warrants on an *ad hoc* basis as they deem fit. Courts must therefore be careful to fill a legislative lacuna only where Parliament has actually failed to anticipate a particular search authorization. The "no other provision" requirement must be interpreted so as to afford the police the flexibility Parliament contemplated in creating the general warrant, while safeguarding against its misuse. There is a need for heightened judicial scrutiny where Parliament has provided an authorization for an investigative technique that is substantively equivalent to what the police seek but

requires more onerous pre-conditions. Thus, the test under s. 487.01(1)(*c*) must consider the investigative technique that the police seek to utilize with an eye to its actual substance and not merely its formal trappings.

The approach to the "no other provision" requirement accepts a measure of uncertainty by tasking judges with the job of inquiring into the substance of purportedly "new" investigative techniques. When uncertainty exists, the police would do well to err on the side of caution. General warrants may not be used as a means to circumvent other authorization provisions that are available but contain more onerous pre-conditions. Judges faced with an application where the investigative technique, though not identical, comes close in substance to an investigative technique covered by another provision for which more rigorous standards apply should therefore proceed with extra caution. Where careful scrutiny establishes that a proposed investigative technique, although similar, has substantive differences from an existing technique, judges may grant the general warrant, mindful of their obligation under s. 487.01(3) to impose terms and conditions that reflect the nature of the privacy interest at stake.

A literal construction of s. 487.01(1)(*c*) must be rejected. Such an approach strips the provision of any meaning and renders it all but valueless. Legislative history confirms that general warrants were to play a modest role, affording the police a constitutionally sound path for investigative techniques that Parliament has not addressed. Ensuring that general warrants are confined to their

limited role is the true purpose of s. 487.01(1)(*c*). While the "best interest" requirement in s. 487.01(1)(*b*) serves to prevent misuse of the general warrant, this provision should not be interpreted as swallowing the distinct analytical question that the "no other provision" test asks. A purposive approach to s. 487.01(1)(*c*) has nothing to do with investigative necessity. Under the "no other provision" test, the police are not asked to show why an alternative authorization would not work on the facts of a particular case, but rather why it is substantively different from what Parliament has already provided.

In this case, the general warrant is invalid because the investigative technique it authorized was substantively equivalent to an intercept. What the police did — securing prospective authorization for the delivery of future private communications on a continual, if not continuous, basis over a sustained period of time — was substantively equivalent to what they would have done pursuant to a Part VI authorization. It was thus, at a minimum, tantamount to an intercept. Though there is no evidence to suggest that the police acted other than in good faith, the police failed to meet their burden to show that the impugned technique was substantively different from an intercept. On the facts here, the general warrant served only to provide a means to avoid the rigours of Part VI. The police could and should have sought a Part VI authorization.

Per McLachlin C.J. and **Cromwell** J. (dissenting): The question of whether what the police did under this general warrant is an interception of a private

communication is one of statutory interpretation. When the text of the statutory provisions is read in its full context, it is clear that the general warrant does not authorize an interception that requires a Part VI authorization. While there is no doubt that the text message is a private communication and that text messages here were intercepted by Telus by means of an electro-magnetic, acoustic, mechanical or other device, the police in this case, did not intercept those messages when Telus turned over to them copies of sent and received messages previously intercepted by Telus and stored in its databases. Therefore, the investigative technique authorized by the general warrant in this case was not an interception of private communication.

Fundamental to both the purpose and to the scheme of the wiretap provisions is the distinction between *the interception* of private communications and *the disclosure, use or retention* of private communications that have been intercepted. The purpose, text and scheme of Part VI show that the disclosure, use or retention of intercepted private communications is distinct from the act of interception itself. That is, if disclosure or use of a private communication were an interception of it, there would be no need to create the distinct disclosure or use offence. Similarly, the exemptions from criminal liability show that Parliament distinguished between interception on one hand and retention, use and disclosure on the other.

In this case, it is not disputed that Telus was intercepting text messages when it copied them for its own systems administration purposes. However, it is also agreed that Telus lawfully intercepted private communications. Under the general

warrant, the police sought disclosure from Telus of information that it had already lawfully intercepted. The general warrant did not require Telus to intercept communications, but to provide copies of communications that it had previously intercepted for its own lawful purposes. As the scheme of the legislation makes clear, disclosure or use of a lawfully intercepted communication is not an interception. It is inconsistent with the fundamental distinction made by the legislation to conclude that the police were intercepting private communications when Telus provided them with copies of previously intercepted and stored text messages. The distinction in the statute between interception and disclosure cannot be dismissed as a mere "technical difference". The distinction is fundamental to the scheme of the provisions. When Telus turns over to the police the copies of the communications that it has previously intercepted, Telus is disclosing the communications, not intercepting them again. This disclosure by Telus from its databases cannot be an interception by the police.

Acquiring the content of a previously intercepted and stored communication cannot be an interception because that broad reading is inconsistent with the clear distinction between interception and disclosure in the provisions. Applied broadly, this interpretation of "acquire" would extend the scope of investigative techniques which require wiretap authorizations far beyond anything ever previously contemplated. Further, introducing a temporal aspect of interception would confuse the act of interception with the nature of its authorization. Interception is a technique, a way of acquiring the substance of a private communication. It could not be that exactly the same technique, which acquires information in exactly the

same form may be either a seizure of stored material or an interception, depending on the point in time at which the technique is authorized.

The general warrant is not one of limited resort that should be used sparingly. On the contrary, as numerous authorities have acknowledged, the provision is cast in wide terms. Therefore, it is not accepted as an imperative that s. 487.01 must be interpreted with a view to heavily restricting its use. The focus of the inquiry is on two matters (in addition of course to reasonable grounds to believe that an offence has been committed and that information concerning the offence will be obtained): is authorization for the "technique, procedure or device to be used or the thing to be done" provided for in any other federal statute and is it in the best interests of the administration of justice to authorize it to be done? Section 487.01(1)(*c*) provides that a general warrant may issue if "there is no other provision . . . that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done". The words "technique", "procedure", "device to be used" and "thing to be done" all are concerned with *what* the police want to do, not *why* they want to do it. This paragraph does not require issuing judges to consider whether other techniques are similar or allow access to the same evidence; it simply asks if the *same technique* can be authorized by another provision. This is not simply a narrow, literal interpretation of s. 487.01. Rather, it is an interpretation that reflects its purpose of conferring a broad judicial discretion to authorize the police to "use any device or investigative technique or procedure or do any thing", provided of course that the judge is satisfied that it is in the best interests

of the administration of justice to do so, having due regard to the importance of the constitutional right to be free of unreasonable searches and seizures. However, courts should not authorize anything the police seek to do simply because it is not authorized elsewhere. The judicial discretion to issue the warrant must give full effect to the protection of reasonable expectations of privacy as set out under s. 8 of the *Charter*.

There is no support in the text or the purpose of s. 487.01(1)(*c*), or in the jurisprudence, for building into it a "substantive equivalency" test. The paragraph asks a simple question: Does federal legislation provide for "a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done"? Where this threshold is met, the judge is entitled to consider granting the requested authorization. The further question of whether the authorization *ought* to be granted is not the focus of this paragraph of the section. Rather, whether a general warrant ought to issue is properly considered under s. 487.01(1)(*b*), which asks whether authorizing the warrant would be in the best interests of the administration of justice. This approach is not only supported by the text, purpose and jurisprudence, but the application of a "substantive equivalency" test creates unnecessary uncertainty and distracts the issuing judge from the question of whether the technique sought to be authorized is inconsistent with the right to be free from unreasonable searches and seizures. Predictability and clarity in the law are particularly important in the area of judicial pre-authorization of searches. The primary objective of pre-authorization is not to identify unreasonable searches after the fact, but to ensure that unreasonable

searches are not conducted. The requirements for pre-authorization should be as clear as possible to ensure that *Charter* rights are fully protected.

The technique sought to be authorized here is not the substantive equivalent of a wiretap authorization. On the facts of this case, a wiretap authorization alone would not allow the police to obtain the information that Telus was required to provide under the general warrant. Three separate authorizations would be required in order to provide the police with the means to access the information provided to them under the general warrant. Therefore, even if one were to accept reading into s. 487.01(1)(*c*) a "substantive equivalency" test, neither the facts nor the law would support its application in this case.

The police did not seek a general warrant in this case as a way to avoid the rigours of Part VI. The general warrant achieved the legitimate aims of the police investigation in a much more convenient and cost-effective manner than any other provision would have allowed. There is no evidence of "misuse" of s. 487.01. The effective and practical police investigation by a relatively small municipal police force was fully respectful of the privacy interests of the targets of the investigation and other Telus subscribers.

Cases Cited

By Abella J.

Referred to: *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. v. Ford*); *R. v. Welsh* (1977), 32 C.C.C. (2d) 363; *Lyons v. The Queen*, [1984] 2 S.C.R. 633; *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992; *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531; *R. v. Wong*, [1990] 3 S.C.R. 36; *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 S.C.R. 427.

By Moldaver J.

Referred to: *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *Lyons v. The Queen*, [1984] 2 S.C.R. 633; *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. v. Ford*); *Schreiber v. Canada (Attorney General)*, [1997] 2 F.C. 176, rev'd [1998] 1 S.C.R. 841; *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992.

By Cromwell J. (dissenting)

Tele-Mobile Co. v. Ontario, 2008 SCC 12, [2008] 1 S.C.R. 305; *R. v. Cole*, 2012 SCC 53; *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241; *R. v. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. v. Cross*, 2007 CanLII 64141; *R. v. Little*, 2009

CanLII 41212; *R. v. Tse*, 2008 BCSC 906, [2008] B.C.J. No. 1766 (QL); *R. v. Weir*, 2001 ABCA 181, 281 A.R. 333; *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, leave to appeal refused, [2009] 3 S.C.R. vii; *R. v. Lauda* (1998), 37 O.R. (3d) 513, aff'd [1998] 2 S.C.R. 683; *R. v. Noseworthy* (1997), 33 O.R. (3d) 641; *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. v. Ford*); *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992.

Statutes and Regulations Cited

Bill C-30, *Protection Children from Internet Predators Act*, 1st Sess., 41st Parl., 2012 (First Reading, February 14, 2012).

Bill C-55, *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, 1st Sess., 41st Parl., 2013 (First Reading, February 11, 2013).

Bill C-176, *Protection of Privacy Act*, 1st Sess., 29th Parl., 1973, Explanatory Note.

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

Criminal Code, R.S.C. 1985, c. C-46, Part VI, ss. 183 "intercept", "private communication", 184, 184.4, 185, 186, 189, 193, 195, 196, 487, 487.01, 487.012, 487.02, 492.2(1), (2).

Criminal Code, S.C. 1993, c. 40, s. 15.

Interpretation Act, R.S.C. 1985, c. I-21, s. 35 "telecommunication".

Protection of Privacy Act, S.C. 1973-74, c. 50.

Authors Cited

Coughlan, Steve. "*R. v. Ha*: Upholding General Warrants without Asking the Right Questions" (2009), 65 C.R. (6th) 41.

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 8th ed. Markham, Ont.: LexisNexis, 2010.

Hutchison, Scott C. *Hutchison's Canadian Search Warrant Manual 2005: A Guide to Legal and Practical Issues Associated with Judicial Pre-Authorization of Investigative Techniques*. Toronto: Thomson Carswell, 2005.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, vol. 1. Toronto: Carswell, 2005 (loose-leaf updated 2012, release 2).

Sullivan, Ruth. *Sullivan on the Construction of Statutes*, 5th ed. Markham, Ont.: LexisNexis, 2008.

Watt, David. *Law of Electronic Surveillance in Canada*. Toronto: Carswell, 1979.

APPEAL from a decision of the Ontario Superior Court of Justice (Sproat J.), 2011 ONSC 1143, 105 O.R. (3d) 411, [2011] O.J. No. 974 (QL), 2011 CarswellOnt 1331, upholding the validity of a general warrant and related assistance order. Appeal allowed, McLachlin C.J. and Cromwell J. dissenting.

Scott C. Hutchison, *Michael Sobkin* and *Fredrick Schumann*, for the appellant.

Croft Michaelson and *Lisa Matthews*, for the respondent.

Michal Fairburn, for the intervener the Attorney General of Ontario.

Wendy Matheson and *Rebecca Wise*, for the intervener the Canadian Civil Liberties Association.

Written submissions only by *Tamir Israel*, for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

The judgment of LeBel, Fish and Abella JJ. was delivered by

ABELLA J. —

[1] For many Canadians, text messaging has become an increasingly popular form of communication. Despite technological differences, text messaging bears several hallmarks of traditional voice communication: it is intended to be conversational, transmission is generally instantaneous, and there is an expectation of privacy in the communication. The issue in this appeal is the proper procedure under the *Criminal Code*, R.S.C. 1985, c. C-46, for authorizing the prospective daily production of these messages from a computer database maintained by a telecommunications service provider.

[2] The service provider in this case is TELUS Communications Company. It urges this Court to find that the prospective, daily acquisition of text messages from their computer database constitutes an interception of private communications and therefore requires authorization under Part VI of the *Code*, a comprehensive scheme for "wiretap authorizations" for the interception of private communications. The Crown, on the other hand, contends that the retrieval of messages from a computer maintained by a service provider does not fall within the scope of Part VI because the

production of messages in computer storage does not amount to an "interception", and that the police are therefore permitted to use the general warrant power in s. 487.01 of the *Code* to get copies of the text messages.

[3] Part VI of the *Code* provides a scheme to protect private communications. Telus employs a unique process for transmitting text messages that results in the messages being stored on their computer database for a brief period of time. The question in this appeal is whether the technical differences inherent in Telus' transmission of text messages should deprive Telus subscribers of the protection of the *Code* that every other Canadian is entitled to.

[4] The focus of this appeal therefore turns on the interpretation of "intercept" within Part VI. "Intercept" is used throughout Part VI with reference to the intercept of *private communications*. This means that in interpreting "intercept a private communication", we must consider the broad scope of Part VI and its application across a number of technological platforms, as well as its objective of protecting individual privacy interests in communications by imposing particularly rigorous safeguards. The interpretation should not be dictated by the technology used to transmit such communications, like the computer used in this case, but by what was intended to be protected under Part VI.

[5] Text messaging is, in essence, an electronic conversation. The only practical difference between text messaging and the traditional voice communications is the transmission process. This distinction should not take text messages outside the

protection of private communications to which they are entitled in Part VI. Technical differences inherent in new technology should not determine the scope of protection afforded to private communications.

Background

[6] When Telus subscribers send a text message, the transmission of that message takes place in the following sequence. It is first transmitted to the nearest cell tower, then to Telus' transmission infrastructure, then to the cell tower nearest to the recipient, and finally to the recipient's phone. If the recipient's phone is turned off or is out of range of a cell tower, the text message will temporarily pause in Telus' transmission infrastructure for up to five days. After five days, Telus stops trying to deliver the message and deletes it without notifying the sender.

[7] Unlike most telecommunications service providers, Telus routinely makes electronic copies of all the text messages sent or received by its subscribers and stores them on a computer database for a period of 30 days. Text messages that are sent by a Telus subscriber are copied to the computer database during the transmission process at the point in time when the text message enters Telus' transmission infrastructure. Text messages received by a Telus subscriber are copied to the computer database when the Telus subscriber's phone receives the message. In many instances, this system results in text messages being copied to the computer database before the recipient's phone has received the text message and/or before the intended recipient has read the text message.

[8] On March 27, 2010, the Owen Sound Police Service obtained a general warrant under s. 487.01 and related assistance order under s. 487.02 of the *Code*. The warrant named two Telus wireless subscribers and required Telus to provide the police with copies of any text messages sent or received by these subscribers which were stored on Telus' computer database. In addition, the warrant required the production of subscriber information identifying any individuals who sent text messages to, or received text messages from the two individuals who were the target of the warrant.

[9] The warrant covered a subsequent two-week period between March 30, 2010 and April 16, 2010. During this time, the warrant required Telus to abide by a specific production schedule. On March 30, 2010, Telus was required to produce the information for March 18, 2010 to March 30, 2010. On each of the following 13 days, Telus was required to produce, on a daily basis, the text messages sent or received within the last 24 hours, as well as any related subscriber information.

[10] Telus argued that the warrant was invalid because the police had failed to satisfy the requirement under s. 487.01(1)(*c*) of the *Code* that a general warrant could not be issued if another provision in the *Code* is available to authorize the technique used by police. Since the warrant purports to authorize the interception of private communications, and since Part VI is the scheme that authorizes the interception of private communications, a general warrant was not available. The Crown's position, on the other hand, was that the retrieval of messages from Telus' computer database

does not fall within the scope of Part VI since the copies on Telus' computer database are not real-time communications and the police are therefore permitted to use the general warrant power to authorize the prospective production of text messages stored on a service provider's computer.

[11] The application judge dismissed Telus' application (2011 ONSC 1143, 105 O.R. (3d) 411). The part of the warrant that required production of historical messages predating the issuance of the warrant was rescinded since both the Crown and Telus conceded that a production order was available to obtain those messages.

[12] In my view, text messages are private communications and, even if they are stored on a service provider's computer, their prospective production requires authorization under Part VI of the *Code*.

[13] If Telus did not maintain its computer database, there is no doubt that the police would be required to obtain an authorization under Part VI to secure the prospective, and in this case continuous, production of text messages. In fact, most service providers do not routinely copy text messages to a computer database as part of their transmission service. Accordingly, if the police wanted to target an individual who used a different service provider, they would have no option but to obtain wiretap authorizations under Part VI to compel the prospective and continuous production of their text messages. This creates a manifest unfairness to individuals who are unlikely to realize that their choice of telecommunications service provider can dramatically affect their privacy.

[14] I would therefore allow the appeal and quash the general warrant and related assistance order.

Analysis

[15] 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.

[16] Section 487.01 was enacted in 1993 as part of a series of amendments to the *Code* in Bill C-109, S.C. 1993, c. 40. The Bill introduced a number of new judicial authorization provisions. Section 487.01 was meant to make search warrants available for techniques or procedures not specified in the *Code*. It authorizes a judge to issue a general warrant permitting a peace officer to "use any device or investigative technique or procedure or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure":

> **487.01** (1) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section,

> use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if
>
> > (*a*) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;
> >
> > (*b*) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and
> >
> > (*c*) *there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.*

[17] The key to this case lies in whether s. 487.01(1)(*c*) applies, namely, whether another provision would provide for the authorization sought in this case. In *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, MacPherson J.A. observed that the focus of the s. 487.01(1)(*c*) analysis is "on the particular investigative technique or procedure that the police seek to utilize and whether it can properly be authorized by another provision in the Code or any other federal statute" (at para. 43; see also *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443, at para. 50 (*sub nom. R. v. Ford*).

[18] Viewed contextually, therefore, s. 487.01(1)(*c*) stipulates that the general warrant power is residual and resort to it is *precluded* where judicial approval for the proposed technique, procedure or device or the "doing of the thing" is available under the *Code* or another federal statute.

[19] In other words, s. 487.01(1)(*c*) should be broadly construed to ensure that the general warrant is not used presumptively. This is to prevent the circumvention of more specific or rigorous pre-authorization requirements for warrants (S.C. Hutchison et al, *Search and Seizure Law in Canada* (looseleaf), at p. 16-40.3).

[20] This means that the Crown is only entitled to a general warrant where it can show that no other provision would provide for a warrant, authorization or order permitting the technique, including, as Moldaver J. observes, provisions that authorize techniques which are substantively equivalent to the technique proposed by the police in a given case. The investigative technique authorized by the general warrant in this case allowed the police to obtain prospective production of future text messages on a daily basis for a two-week period directly from a service provider. The essence of the Crown's argument was that no other provision was available because the retrieval of stored messages was not an interception. If the Crown is right, they are entitled to a general warrant. If they are wrong, the general warrant must be quashed. Either way, it is impossible to avoid an examination of whether the technique the police sought to employ was something that required a Part VI authorization.

[21] The Crown never conceded that these were circumstances in which a choice was available under either a general warrant or a Part VI authorization. Instead, it argued that the requirement in s. 487.01(1)(*c*) was satisfied because no

other provision was available to authorize the prospective production of future text messages stored on a service provider's computer, maintaining that Part VI did not apply because the retrieval of messages from computer storage is not an "intercept". That is the central issue that is engaged in this case.

[22] This requires us to determine whether Part VI applies to the prospective, and in this case continuous, production of text messages sought by the police, or whether the fact that the messages are stored in Telus' computer means that their retrieval by the police is not an "intercept". If Part VI does apply, then in accordance with s. 487.01(1)(*c*), a general warrant is not available.

[23] Section 184(1) makes it an indictable offence to "wilfully intercep[t] a private communication" by use of a device. Part VI provides a comprehensive scheme for the authorization of these interceptions. It was enacted in 1974 through the *Protection of Privacy Act*, S.C. 1973-74, c. 50, which amended the *Code* to add Part IV.1 (now Part VI) entitled "Invasion of Privacy". The goal of the legislation was explained by Zuber J.A. in *R. v. Welsh* (1977), 32 C.C.C. (2d) 363 (Ont. C.A.) as follows:

> It is apparent that in enacting the *Protection of Privacy Act*, 1973-74 (Can.), c. 50, . . . Parliament had two objectives. The first was to protect private communications by prohibiting interception and to render inadmissible evidence obtained in violation of the statute. The second objective, which balances the first, was to recognize the need to allow the appropriate authorities, subject to specific controls, to intercept private communications in the investigation of serious crime, and to adduce the evidence thus obtained. [p. 369]

[24] Because the purpose of Part VI is to restrict the ability of the police to obtain and disclose private communications, it is drafted broadly to ensure the necessary protection. In *Lyons v. The Queen*, [1984] 2 S.C.R. 633, this Court explained this breadth as follows:

> This is broad legislation embracing in these extensive provisions the use of a wide range of radio, telephone, optical and acoustical devices for listening to and recording private communications as broadly defined. It is not "wiretapping" legislation, nor eavesdropping legislation, nor radio regulation. It is the regulation of all these things and "any other device" that may be used to intercept intelligence reasonably expected by the originator not to be intercepted by anyone other than the intended recipient. [p. 664]

[25] The definition of "intercept" in s. 183 includes "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof". Consistent with the broad scope of Part VI, this definition is not exhaustive and focuses on the state acquisition of informational content — the substance, meaning, or purport — of the private communication. It is not just the communication itself that is protected, but any derivative of that communication that would convey its substance or meaning. "[P]rivate communication" is defined in s. 183 as follows:

> . . . *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;

[26] This definition focuses on the individual's reasonable expectation of privacy in the communication. The word "telecommunication" used in this definition is in turn defined in the *Interpretation Act*, R.S.C., 1985, c. I-21, s. 35, amended in 1993 (S.C. 1993, c. 38, s. 87) 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".

[27] Sections 185 and 186 of the *Code* set out the general requirements governing the application for an authorization under Part VI. Compared with other search and seizure and warrant provisions in the *Code*, the provisions in Part VI contain more stringent requirements to safeguard privacy interests. Before granting an authorization under Part VI, a judge must be satisfied that the authorization is in the best interests of the administration of justice.

[28] A judge must also be satisfied, in accordance with s. 186(1)(*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". In *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, this Court clarified that this criterion required the police to show that there was "no other reasonable alternative method of investigation in the circumstances of the particular criminal inquiry" (para. 29).

[29] Part VI authorizations must also state the identity of persons whose private communications will be intercepted, the place at which they are intercepted, and the manner of the interception. They are required to contain such conditions as the judge considers advisable and will only be valid for a limited period of time not to exceed 60 days. Finally, a written application by the Attorney General, Minister of Public Safety or a designated agent is required.

[30] In addition to these prerequisites for authorization, Part VI contains a number of notice requirements. Section 196 requires that notice be given to targets of interceptions authorized under s. 186 within a certain timeframe. Under s. 189, an accused must be given notice of any interception intended to be produced in evidence. In addition, s. 195 requires the Minister of Public Safety and Emergency Preparedness or the Attorney General for each province to produce an annual report with respect to the use of Part VI authorizations. In *R. v. Tse*, 2012 SCC 16, [2012] 1 S.C.R. 531, this Court found that a notice requirement provides transparency and serves as a further check on the power of police to perform highly intrusive interceptions of private communications. The Court therefore concluded that a notice provision was necessary to meet the minimal constitutional standards of s. 8 of the *Canadian Charter of Rights and Freedoms*.

[31] These safeguards illuminate Parliament's intention that a higher degree of protection be available for private communications. Part VI has broad application to a number of technologies and includes more rigorous safeguards than other warrant

provisions in the *Code*. In considering whether the prospective, daily production of future text messages stored in Telus' computer falls within Part VI, therefore, we must take this overall objective into account.

[32] As all parties acknowledged, it is clear that text messages qualify as telecommunications under the definition in the *Interpretation Act*. They also acknowledged that these messages, like voice communications, are made under circumstances that attract a reasonable expectation of privacy and therefore constitute "private communication" within the meaning of s. 183. Similarly, there is no question that the computer used by Telus would qualify as "any device" under the definitions in s. 183.

[33] The issue then is how to define "intercept" in Part VI. The interpretation should be informed not only by the purposes of Part VI, but also by the rights enshrined in s. 8 of the *Charter*, which in turn must remain aligned with technological developments. In *R. v. Wong*, [1990] 3 S.C.R. 36, this Court found that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 [of the *Charter*] is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take" (p. 44). A technical approach to "intercept" would essentially render Part VI irrelevant to the protection of the right to privacy in new, electronic and text-based

communications technologies, which generate and store copies of private communications as part of the transmission process.

[34] It is true that unlike traditional voice communication, a text message may or may not be delivered to its intended recipient at the time it is created. Receipt of the text message depends on whether the phone is turned on, whether it is in range of a cell tower, and whether the user has accessed the message. If Telus is unable to deliver the message, it remains in the transmission infrastructure for five days, at which point Telus stops trying to complete delivery. Furthermore, unlike voice communications, text communications, by their nature, generate a record of the communication which may easily be copied and stored. A narrow or technical definition of "intercept" that requires the act of interception to occur simultaneously with the making of the communication itself is therefore unhelpful in addressing new, text-based electronic communications.

[35] A narrow definition is also inconsistent with the broad language and purpose of Part VI. The statutory definition of "intercept" in s. 183 includes three distinct parts — "listen to", "record" *or* "acquire". In French, the definition includes "*de prendre . . . connaissance*". Rather than limit the definition of "intercept" to its narrow, technical definition, the statutory definition broadens the concept of interception. There is no requirement in the *Code* definition of "intercept" that the interception of a private communication be simultaneous or contemporaneous with the making of the communication itself. If Parliament intended to include such a

requirement, it would have included it in the definition of "intercept". Instead, it chose to adopt a wider definition, consistent with Part VI's purpose to offer broad protection for private communications from unauthorized interference by the state.

[36] The interpretation of "intercept a private communication" must, therefore, focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made. In my view, to the extent that there may be any temporal element inherent in the technical meaning of intercept, it should not trump Parliament's intention in Part VI to protect an individual's right to privacy in his or her communications.

[37] The use of the word "intercept" implies that the private communication is acquired in the course of the communication process. In my view, the process encompasses all activities of the service provider which are required for, or incidental to, the provision of the communications service. Acquiring the substance of a private communication from a computer maintained by a telecommunications service provider would, as a result, be included in that process.

[38] Focusing on the fact that the *Code* draws a distinction between the interception of private communications and the disclosure of those communications, fails to provide the intended protection under Part VI. On the contrary, it allows technological differences in Telus' transmission process to defeat Parliament's intended protection of private communications from state interference.

[39] The reality of modern communication technologies is that electronic private communications, such as text messages, are often simultaneously in transit *and* in some form of computer storage by the service provider. As a result, the same private communication exists in more than one place and may therefore be acquired by the state from the transmission stream and from computer storage. In other words, the same private communication may be "intercepted" by police more than once from different sources.

[40] When Telus copies messages to its computer database, several steps in the transmission process have yet to occur. The production schedule required by the general warrant in this case means that the police likely obtained stored copies of some text messages before they were even received by the intended recipient. Had the police acquired the same private communications directly from the transmission stream, instead of from the stored copies, the Crown concedes that a Part VI authorization would be required. The level of protection should not depend on whether the state acquires a copy of the private communication that is being transmitted or a copy that is in storage by a service provider as part of the communications process. Parliament drafted Part VI broadly to ensure that private communications were protected across a number of technological platforms (see *Lyons*).

[41] The communication process used by a third-party service provider should not defeat Parliament's intended protection for private communications. As the

interveners Canadian Civil Liberties Association and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic point out in their factums, this Court has recognized in other contexts that telecommunications service providers act merely as a third-party "conduit" for the transmission of private communications and ought to be able to provide services without having a legal effect on the nature (or, in this case, the protection) of these communications (*Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, 2004 SCC 45, [2004] 2 S.C.R. 427, at paras. 100-101).

[42] Part VI recognizes the dangers inherent in permitting access to the future private communications of a potentially unlimited number of people over a lengthy period of time. Those are the very risks inherent in the investigative technique in this case. An authorization that permits police to obtain the *prospective* production of *future* text messages over a two-week period directly from the communications process used by the service provider is precisely what Part VI was intended to protect. In my view, the investigative technique in this case therefore qualifies as "intercepting private communications" under Part VI.

[43] An interpretation of "intercept a private communication" that includes the investigative technique used by police in this case finds support in the statutory definition of "intercept" in s. 183. The definition includes the simple acquisition of a communication. It does not require the acquisition of the communication itself; rather, the acquisition of the "substance, meaning or purport" of the communication is

sufficient. Moreover, this interpretation is harmonious with the scheme and objectives of Part VI, which is drafted broadly in order to regulate and control a wide variety of technological invasions of privacy. Finally, it strikes the appropriate balance between the serious invasion of privacy that results from the surreptitious acquisition of private communications and the evolving needs of effective law enforcement.

[44] The police gained a substantial advantage by proceeding with a general warrant. They did not need the Attorney General's request for an authorization; they did not need to show that other investigative procedures had been tried and failed; they did not need to provide any notice to the target individuals; and they did not need to identify which other individuals' private communications may be acquired in the course of the search.

[45] The general warrant in this case purported to authorize an investigative technique contemplated by a wiretap authorization under Part VI, namely, it allowed the police to obtain *prospective* production of *future* private communications from a computer maintained by a service provider as part of its communications process. Because Part VI applied, a general warrant under s. 487.01 was unavailable.

[46] Accordingly, I would allow the appeal and quash the general warrant and related assistance order.

The reasons of Moldaver and Karakatsanis JJ. were delivered by

MOLDAVER J. —

I. Introduction

[47] Where a police investigative technique intrudes on an individual's reasonable expectation of privacy, it falls to Parliament to provide for specific legislative authorization of the technique. That is the general rule. The so-called "general warrant" provision of the *Criminal Code*, R.S.C. 1985, c. C-46, operates as an exception to the rule, allowing the police to seek judicial authorization of a proposed investigative technique that is not specifically authorized by statute. Although several issues have been raised in this appeal, the dispositive one, in my view, is whether a general warrant may properly issue where the substance of an investigative technique, if not its precise form, is addressed by an existing legislative provision.

[48] I have had the benefit of reading the reasons of my colleague Abella J. and, although we approach the matter differently, I share her conclusion that the general warrant in this case is invalid. My colleague's reasons focus on the definition of "intercept" in s. 183 of the *Code* and whether the search in this case fell within that definition for purposes of Part VI. I do not think it necessary to answer those questions because in my view the result in this case is driven by the failure of the authorities to establish one of the prerequisites needed to obtain a general warrant.

[49] On the facts of this case, when one cuts through form and looks at the substance of the search that the police sought to conduct, what we are left with is the equivalent of a Part VI intercept. As such, the police could and, for reasons I will explain, should have sought an authorization under Part VI, which thereby precludes the issuance of a general warrant. I would accordingly join my colleague Abella J. in allowing the appeal and quashing the general warrant, as well as the related assistance order.

II. Overview of Issues on Appeal

[50] The parties in this appeal framed their principal arguments around the question of whether the investigative technique authorized by the general warrant falls within the definition of "intercept" in s. 183 of the *Code*. The parties agree that if what occurred here was an intercept, the general warrant could not issue, as it would fail the "no other provision" requirement in s. 487.01(1)(*c*) of the *Code*. They, of course, disagree as to whether this technique was an intercept.

[51] My colleague Abella J. and I agree that the Crown is entitled to a general warrant only where it can show that "no other provision" would provide for the technique, including a substantively equivalent technique, proposed by the police in a given case. We also agree on the result in this case. We part company, however, on the path to that result.

[52] My colleague takes the position that the investigative technique here *was* an intercept within the meaning of s. 183, and would thereby hold the general warrant invalid. I prefer, instead, to resolve this case on the basis that the investigative technique here *was substantively equivalent* to an intercept and, in light of that conclusion, would hold the general warrant invalid.

[53] I choose a different path because I am reluctant to use this case as a vehicle to undertake an analysis of what constitutes an intercept for purposes of Part VI. 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.

III. Analysis

A. *The General Warrant Provision*

[54] Parliament enacted the general warrant provision in 1993 together with several new search powers as part of its response to a series of decisions of this Court concerning electronic surveillance. Section 487.01 was a specific response to *R. v. Wong*, [1990] 3 S.C.R. 36. That decision held that police video monitoring of

activities in a hotel room intruded on an individual's reasonable expectation of privacy and thus required prior judicial authorization pursuant to a valid legislative provision. Parliament's response, in the form of s. 487.01, went beyond the authorization of video monitoring. The provision states in relevant part:

> **487.01** (1) [Information for general warrant] A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if
>
> (*a*) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;
>
> (*b*) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and
>
> (*c*) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.
>
> (2) [Limitation] Nothing in subsection (1) shall be construed as to permit interference with the bodily integrity of any person.
>
> (3) [Search or seizure to be reasonable] A warrant issued under subsection (1) shall contain such terms and conditions as the judge considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances.

[55] The breadth of the general warrant — judicial sanction to "use any device or investigative technique or procedure or do any thing" that if not authorized would constitute an unreasonable search or seizure — is kept in check by several

prerequisites to its availability and conditions on its operation. Chief among them and what, in my view, lies at the heart of this appeal is the requirement in s. 487.01(1)(*c*) that "there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done".

[56] The requirement that there be "no other provision" that would provide for the search ensures that the general warrant is used sparingly as a warrant of limited resort. It guards against the general warrant becoming "an easy back door for other techniques that have more demanding pre-authorization requirements": S. C. Hutchison et al, *Search and Seizure Law in Canada* (loose-leaf), at p. 16-40.3. Without ascribing any improper motive to the police, that, I believe, is what occurred in this case.

B. *The General Warrant in This Case*

[57] In a typical scenario where TELUS Communications Company ("Telus"), the telecommunications service provider here, is served with an authorization under Part VI, the company installs a device that automatically copies all activity for the identified phone number, including all text messages, and automatically delivers such data to a police "wire room". The Crown does not dispute that the acquisition of an individual's text messages in this manner constitutes a Part VI intercept, nor is there any dispute that a text message can constitute a "private communication" within the meaning of Part VI.

[58] As a matter of corporate practice, however, Telus routinely stores a copy of a subscriber's incoming and outgoing text messages on its databases for at least 30 days. Though Telus is unique among major telecommunications service providers in making such copies, it is legally entitled to do so pursuant to an exception in s. 184(2) of the *Code*. The company says it intercepts its subscribers' messages in this manner to aid in troubleshooting customer problems.

[59] The fact that Telus stores its subscribers' text messages in this manner is significant — indeed, it is the reason this appeal exists — because it creates an investigative resource for the authorities. As Det. Sgt. Prosser of the Ontario Provincial Police said in his affidavit filed with this Court, Telus's practice "provides investigators with another option by which to access the content of these messages" (A.R., at p. 115). Relying on conventional search warrants (s. 487) or production orders (s. 487.012), the police have obtained copies of the messages stored in Telus's databases.

[60] In sum, prior to this case, with only a handful of exceptions, all police searches that sought copies of Telus subscribers' text messages were authorized either under Part VI or by a conventional search warrant or production order. The Crown in its factum puts the matter succinctly: police practice with respect to Telus subscribers has been to seek either "search warrants or production orders (<u>for historic messages</u>) or wiretap authorizations (<u>for future messages</u>)" (R.F., at para. 10 (emphasis added)).

[61] The general warrant in this case thus represents a third option. In form, it resembles a production order because it authorizes police access to text messages *already stored in Telus's database*. And yet, in substance, it resembles a Part VI authorization, because it *prospectively* authorizes police access to *future* private communications on a *continual* basis over a sustained period of time.

[62] The inherent hybridity of the general warrant in this case underscores the need for an inquiry into whether the "no other provision" test is satisfied to assess the substance of the police investigative technique, not merely its formal trappings. But that is not what happened here.

C. *Was the General Warrant Validly Issued?*

[63] The reviewing judge looked to binding authority from the Ontario Court of Appeal for guidance. In *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, MacPherson J.A. observed:

> The focus in the s. 487.01(1)(*c*) analysis is not on whether there are other investigative techniques that might accomplish the purported investigative purposes or goals of the police; rather, the focus is on the particular investigative technique or procedure that the police seek to utilize and whether it can properly be authorized by another provision in the Code or any other federal statute. [Emphasis added; para. 43.]

[64] On the strength of *Ha*, the reviewing judge concluded that there was no other provision in the *Code* or any other statute that would authorize the investigative

technique in this case — namely the "prospective and daily production of text messages" (2011 ONSC 1143, 105 O.R. (3d) 411, at para. 75). Though the police "could have gone to a justice of the peace every day for the 14 days covered by the General Warrant and obtained the same records using conventional warrants", the general warrant could issue precisely because it provided a single, comprehensive authorization for the search that was otherwise unanticipated by Parliament (para. 70).[1]

[65] The analysis is, in my respectful view, incomplete. It is self-evident that the police *could* have sought a Part VI authorization and achieved their investigative objective. Crown counsel recognized this during the hearing of this appeal:

> I'm not sure that they really thought this through at the end of the day because if what the police are doing here is Part VI, well, you know, presumably, the police could go back to the issuing justice who was a Superior Court judge and say: Okay. Just issue this as a Part VI authorization. [Emphasis added; transcript, at p. 81.]

On the record before us, the police have offered no explanation as to why they could not have sought a Part VI authorization. We do know that but for Telus's practice of routinely storing subscribers' messages, the police would have had no option other than to obtain such an authorization since what they were seeking was prospective authorization for the daily production of future text messages. Indeed, that is what they do — ostensibly without any trouble — with the other major

[1] The validity of a series of daily (or more frequent) production orders was not argued by the parties, nor is addressing that issue necessary to resolve this appeal. Accordingly, I would not decide whether there exists any statutory or constitutional bar to the police seeking such orders.

telecommunications service providers, such as Rogers and Bell, who do not store text messages as Telus does.

[66] Nonetheless, the question remains whether the law requires that the police *should* have sought such an authorization. At the hearing of this appeal, Crown counsel argued that *Ha* conclusively resolves the issue in the negative:

> [A]s the Ontario Court of Appeal pointed out in Ha, the test for determining whether a general warrant can be issued focuses on the nature of the investigative technique in question, not the nature of the investigative objective.
>
> The search of the Telus database for future records is a technique that's quite distinct from the seizure of a telecommunication. I mean, mechanically, the police were doing different things. It was a completely different process. [Emphasis added; transcript, at pp. 94-95.]

[67] With respect, I cannot agree. To adopt *Ha* in this way is to turn a blind eye to the substance of the search — and to common sense. What the police did in this case — securing *prospective* authorization for the delivery of *future* private communications on a *continual*, if not continuous, basis over a sustained period of time — was substantively equivalent to what they would have done pursuant to a Part VI authorization. It was thus, at a minimum, tantamount to an intercept.

[68] I accept the Crown's contention that, as a technical matter, what occurred here was different from what would occur pursuant to a Part VI authorization. I do not accept, however, that that fact is determinative in light of the identical privacy interests at stake. But for the 24-hour time delay, the investigative techniques were

the same. Indeed, if the Crown's logic is to be accepted, a general warrant could still issue had the delay been 24 minutes or, for that matter, 24 seconds.[2] To draw a line between what was authorized here and a Part VI intercept on the basis of such a theory is to draw "an artificial and unrealistic distinction": *Lyons v. The Queen*, [1984] 2 S.C.R. 633, at p. 643.

[69] As a result, the facts of the case at hand are distinguishable from *Ha*. Both *Ha* and *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. v. Ford*), the other appellate authority interpreting s. 487.01, concerned unsuccessful attempts by the target of a search to invalidate a general warrant on the basis that the police could have sought multiple conventional warrants. In *Ha*, the police were investigating a suspected drug lab. They sought the flexibility to enter the property covertly at any time within a two-month period and to engage in a broad range of evidence gathering activities therein, including photographing, taking chemical samples, and fingerprinting items. Likewise, in *Brand*, the police were investigating a large marihuana grow operation and needed covert access to multiple properties in order to verify the presence of drugs without compromising other aspects of their investigation. Fundamentally, in each instance, the request for covert access and temporal flexibility made clear that the *substance* of the investigative techniques for

[2] It is neither prudent nor necessary to draw a bright line in this case as to when the period of delay would render the search technique substantively different such that a general warrant would be acceptable. Whatever that timeframe may be, the 24-hour gap here fell short of the mark. To the extent that uncertainty arises in a future case, it must be resolved in keeping with the approach to s. 487.01(1)(*c*) articulated here. I also note that my colleague Cromwell J. makes much of the fact that "some of the messages that police were to receive would be delayed by 72 hours, not 24" (para. 183). With respect, I find his emphasis on this fact puzzling. Even if one assumes that a 72-hour delay is substantively different from an intercept, it hardly follows that because one part of an otherwise offensive authorization is valid, the entire authorization should be spared.

which authorization was sought differed from what could be authorized under a conventional warrant.

[70] Explaining why the search sanctioned by the general warrant in *Ha* was thus substantively different from one involving multiple conventional warrants, MacPherson J.A. said:

> In this case, the police sought to obtain authorization to conduct an unlimited number of covert entries and searches on private property over a two-month period. Except for s. 487.01 of the Code, there is "no other provision in . . . any other Act of Parliament" that could potentially accomplish this goal. [para. 43]

Those are not our facts. Here, the police sought, in the reviewing judge's words, authorization for "the investigative technique or procedure of prospective and daily production of text messages" (para. 75). The simple fact is there *is* a provision that substantively provides for this technique. It is known as Part VI.

[71] In emphasizing the importance of looking beyond the form of a search technique to uncover its true substance, a further point bears noting. In both *Ha* and *Brand*, if the police wanted the evidence, they had a choice between a series of conventional warrants or a general warrant. If the police sought a general warrant, they would have to meet the requirements of s. 487.01 which are deliberately stricter than those for a conventional warrant. For example, the requirements that a general warrant can only be issued by a judge, not a justice of the peace, and that issuance

must be in the best interests of justice themselves serve to ensure that the general warrant remains a rearguard warrant of limited resort.

[72] In other words, by dint of its more stringent requirements, the general warrant contains a disincentive to its everyday use. In *Ha* and *Brand*, where the only alternative was a series of conventional warrants, reliance on a general warrant did not provide the police with an easy way out from the rigours of a more demanding legislative authorization — the general warrant *was* the more demanding legislative authorization. Thus, in these cases, it is harder to see how the general warrant provision might be misused.

[73] In this case, by contrast, the police actually had a choice between a Part VI authorization and a general warrant.[3] The incentives before the police were thus markedly different than they were in *Ha*. Though both the general warrant and the Part VI provisions require that the issuing judge be satisfied that the order is in the best interests of justice, Part VI alone imposes several further requirements in the interest of protecting the right to privacy:

1. An authorization under Part VI is available only for certain offences (s. 183).

[3] The record in this case suggests that the entirety of the information sought by the police could have been obtained pursuant to a Part VI authorization, a number recorder under s. 492.2(1), and an order to obtain telephone records under s. 492.2(2). Before this Court, none of the parties concentrated on the latter two authorizations; rather, they focused on whether the warrant's core — the delivery of text messages — amounted to an intercept.

2. Only individuals designated by the Minister of Public Safety and Emergency Preparedness or Attorney General may seek a Part VI authorization (ss. 185(1), 186(6)).

3. A Part VI authorization is available only where "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" (s. 186(1)(*b*)).

4. A Part VI authorization must state the identity of persons whose private communications will be intercepted, the place at which they are intercepted, and the manner of the interception (s. 186(4)(*c*)).

5. The Attorney General or Minister is required to provide notice to the target of the authorization within a certain timeframe (s. 196).

6. The Minister is required to make an annual report to Parliament concerning the number of applications made for authorizations under Part VI and the details thereof (s. 195).

[74] Consequently, in this case, a narrow focus on the mechanics of the search is to miss the forest for the trees. The general warrant must be analogized to a Part VI

authorization if one is to appreciate the actual incentives before the police. A mechanistic interpretation of the "no other provision" requirement cannot hold because, put bluntly, a general warrant can prove easier to obtain than a Part VI authorization. For that reason, one can hardly fault the police for seeking a general warrant instead of a Part VI authorization. There was little to be lost (a delay in the receipt of the data sought, which may well have had little consequence) and much to be gained (no requirement to meet the onerous burdens Parliament has chosen to impose under Part VI).

[75] The facts suggest that this is precisely what has happened as a consequence of Telus's unsuccessful challenge of the warrant in this case. The affidavit of Det. Sgt. Prosser states that the police seek general warrants only in those "rare circumstances" requiring access to text messages "under a more immediate timeline" (A.R., at p. 116). And yet, though Telus received only six general warrants prior to 2010, counsel for the company informed us at the hearing of this appeal that the number has since grown to "several hundred" in light of the decision below (transcript, at p. 42).

[76] The logic that led to this predictable result effectively nullifies the "no other provision" safeguard by inviting the police to distinguish an investigative technique in some manner — any manner, even if substantively immaterial — so as to avoid the rigours of a more demanding legislative authorization such as Part VI. Faced with the choice of having to seek an authorization under Part VI and being able

to proceed down a less demanding path, it should be expected that the police will elect the latter — and understandably so. It follows, in my view, that the "no other provision" test must be given interpretive teeth if it is to serve its purpose of ensuring that general warrants do not become a means to avoid more onerous search authorizations.

D. *Summary of the Approach to the "No Other Provision" Requirement*

[77] The test under s. 487.01(1)(*c*) must consider the investigative technique that the police seek to utilize with an eye to its actual substance and not merely its formal trappings. The provision must be interpreted so as to afford the police the flexibility Parliament contemplated in creating the general warrant, while safeguarding against its misuse. As the facts of this case illustrate, there is a need for heightened judicial scrutiny where Parliament has provided an authorization for an investigative technique that is substantively equivalent to what the police seek but requires more onerous pre-conditions.

[78] In so concluding, I note that in creating the general warrant, Parliament did not erase every other search authorization from the *Code* and leave it to judges to devise general warrants on an *ad hoc* basis as they deem fit. Courts must therefore be careful to fill a legislative lacuna only where Parliament has actually failed to anticipate a particular search authorization. To do otherwise would chip away at the foundation that shapes the respective roles of the courts and Parliament in our system of criminal justice when individual rights and freedoms are at stake.

[79] That said, I recognize, as I must, that this approach accepts a measure of uncertainty by tasking judges with the job of inquiring into the substance of purportedly "new" investigative techniques. In my view, an interpretation that is faithful to the purpose of the "no other provision" requirement in s. 487.01(1)(*c*) necessarily demands as much. Two practical guidelines, however, should serve to mitigate concerns that may arise.

[80] First, it is important for the police to appreciate that general warrants are not warrants of general application. On the contrary, they are to be used sparingly, when the investigative technique they wish to employ is truly different in substance from an investigative technique accounted for by another legislative provision. Where uncertainty exists, the police would do well to err on the side of caution. They must know — with certainty — that general warrants may not be used as a means to circumvent other authorization provisions that are available but contain more onerous pre-conditions.

[81] Second, when judges are faced with an application for a general warrant where the investigative technique, though not identical, comes close in substance to an investigative technique covered by another provision for which more rigorous standards apply, they should proceed with extra caution. At a minimum, judges should look closely at the material filed and satisfy themselves that the request for a general warrant is genuine and not merely a device to escape the rigours of another authorization provision. Where careful scrutiny establishes that a proposed

investigative technique, although similar, has *substantive* differences from an existing technique — not simply that it is similar in substance but different in form — judges may grant the general warrant, but they should be mindful of their obligation under s. 487.01(3) to impose terms and conditions that reflect the nature of the privacy interest at stake. In doing so, they may borrow as appropriate from the conditions that Parliament has chosen to impose on the substantively similar existing authorization.

[82] With these twin considerations in mind, and despite Justice Cromwell's concerns about certainty, to which I shall turn momentarily, if the police proceed in good faith and the authorizing judge proceeds with caution, it is unlikely that a general warrant issued in such circumstances will be found to be defective at trial — and even less so that evidence obtained pursuant to it will be excluded under s. 24(2) of the *Canadian Charter of Rights and Freedoms*.

E. *The Competing Approach to the "No Other Provision" Requirement*

[83] I have had the opportunity to read the reasons of Cromwell J., who is of the view that the "no other provision" test was satisfied in this case because the investigative technique does not meet the definition of "intercept" for purposes of Part VI. He would accordingly dismiss the appeal. Insofar as the definition of an intercept is concerned, my colleague's analysis hinges on distinguishing between the interception of a private communication (s. 184) and the subsequent disclosure of such intercepted communications (s. 193). As I have explained, I do not find it

necessary to reach that question in this appeal and, for that reason, do not comment on this aspect of his reasons.

[84] My colleague does, however, take issue with my interpretation of s. 487.01(1)(*c*) and its application to the case at hand. It is clear that my colleague and I have fundamentally different understandings not only of the "no other provision" requirement, but the proper role of general warrants more broadly. He has offered a careful analysis that warrants a response.

[85] Justice Cromwell maintains that s. 487.01(1)(*c*) should be construed literally and he rejects the purposive approach I have taken, asserting that it "creates unnecessary uncertainty and distracts the issuing judge from the question of whether the technique sought to be authorized is inconsistent with the right to be free from unreasonable searches and seizures" (para. 171). According to my colleague, "predictability and clarity in the law are particularly important in the area of judicial pre-authorization of searches" (para. 172).

[86] Justice Cromwell further challenges my construction of s. 487.01(1)(*c*) on the basis that it impermissibly adds "investigative necessity" as a further pre-condition to the issuance of a general warrant — that is, to obtain a general warrant, the police must be able to show that there are no other ways by which they can achieve their investigative objective. My colleague maintains that Parliament did not see fit to add such a requirement and it is impermissible for the Court to do so.

[87] I propose to address each of Justice Cromwell's concerns.

[88] First, for reasons that should be clear from the above, I cannot accept my colleague's literal construction of s. 487.01(1)(*c*). With respect, such an interpretation strips the provision of any meaning and renders it all but valueless. Writing in 1996, soon after the general warrant was introduced, the authors of a leading treatise on this subject predicted:

> Of the four preconditions [to a general warrant] the most difficult for investigators will be [the "no other provision" requirement], a novel provision intended to prevent this residual warrant power from becoming an easy back door for other techniques that have more demanding pre-authorization requirements. [Emphasis added; Hutchison et al, at p. 16-40.3.]

My colleague's approach, however, would reduce that provision to a paper tiger.

[89] On my colleague's literal interpretation of s. 487.01(1)(*c*), any deviation — no matter how slight or insignificant — that takes an investigative technique outside the four corners of another authorization provision in the *Code* or an Act of Parliament is sufficient to satisfy the "no other provision" requirement. Thus, in this case, had the police sought a general warrant requiring Telus to provide copies of all stored text messages using a 24-second delay (as opposed to a 24-hour delay), I gather that my colleague would hold that the "no other provision" requirement had been met. Likewise, on my colleague's construction, had the police sought a general warrant requiring both the *contemporaneous* interception of text messages *and* a dial

number recorder warrant, it would appear that this too would suffice to satisfy the "no other provision" requirement.

[90] If, as my colleague reasons, Parliament truly intended that the police could satisfy the "no other provision" requirement by coming up with a hook — any hook — that would take the investigative technique outside the four corners of an existing authorization, then we are left to conclude that Parliament chose to enact an absurdity. I cannot accept any such conclusion.

[91] Moreover, my colleague's focus on the breadth of the general warrant provision — breadth that I readily accept — conflates the distinct questions of *what* the power can do, assuming it is available, with *when* it arises. As I have already observed, the general warrant provision was not meant to erase every other authorization provision from the *Code* and leave it to individual judges to fashion general warrants on an *ad hoc* basis. On the contrary, general warrants were created "to fill any potential 'gap'" (*Schreiber v. Canada (Attorney General)*, [1997] 2 F.C. 176, at para. 86 (emphasis added), rev'd on other grounds, [1998] 1 S.C.R. 841), to provide a "legislative 'failsafe'" that "supplement[s] rather than supplant[s]" (Scott C. Hutchison, *Hutchison's Canadian Search Warrant Manual 2005* (2005), at pp. 143 and 163 (emphasis added)), to "fill an investigatory hiatus" (J. A. Fontana and D. Keeshan, *The Law of Search and Seizure in Canada* (8th ed. 2010), at p. 459 (emphasis added)), and to serve as a "residual power" (Hutchison et al, at p. 16-36 (emphasis added)).

[92] Though little was said of general warrants in debates or committee hearings in 1993, we do know that Parliament did not get out of the warrant business after enacting s. 487.01. Multiple new authorizations have been created since then, including production orders in 2004. Existing authorizations have been amended to reflect evolving investigatory needs and privacy concerns, including the provisions of Part VI. And even today Parliament continues to consider warrant proposals introduced — and sometimes withdrawn — by the government. See, e.g., Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess., 41st Parl., (First Reading, February 14, 2012); Bill C-55, *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, 1st Sess., 41st Parl., (First Reading, February 11, 2013).

[93] This history confirms that general warrants were to play a modest role, affording the police a constitutionally sound path for investigative techniques that Parliament had not addressed. They were thus rearguard warrants of limited resort, not frontline warrants of general application. They were meant to fill gaps, not create them.

[94] In sum, ensuring that general warrants are confined to their limited role, in my view, is the true purpose of s. 487.01(1)(*c*). Justice Cromwell's literal construction of the provision turns that purpose on its head by inviting the police to seek judicial sanction of purportedly "new" investigative techniques on the basis of substantively meaningless distinctions. Manifestly, this approach puts a premium on form over substance.

[95] My colleague takes comfort in the "best interests" clause in s. 487.01(1)(*b*) as an adequate safeguard against misuse of the general warrant. Parliament, he contends, enacted subsection (1)(*b*) to deal alone with "potential abuses of the general warrant" (para. 190). But if that is so, one might ask why Parliament enacted s. 487.01(1)(*c*) in the first place.

[96] No doubt, the "best interests" requirement serves to prevent misuse of the general warrant. But this provision should not be interpreted as swallowing the distinct analytical question that the "no other provision" test asks. The role of each provision must be respected. First, under s. 487.01(1)(*c*), the question is whether there is any other provision in the *Code* or other Act of Parliament that actually or substantively provides for the investigative technique for which the police seek authorization. Second, under s. 487.01(1)(*b*), only if the first question is answered in the negative does the inquiry shift to whether issuance of the warrant is in the best interests of the administration of justice.

[97] The two hypotheticals I mentioned earlier illustrate the point. I would hope that a 24-second delay and a dial number recorder warrant piggy-backed on an authorization for the contemporaneous interception of text messages would meet my colleague's definition of abuse. Why? Because both investigative techniques would presumably be seen for what they are — the substantive equivalent of a Part VI authorization. In the end, all roads lead to Rome. But the interpretation of s.

487.01(1)(*c*) that I endorse gives some meaning and purpose to the provision; my colleague's interpretation strips it of both.

[98] Insofar as s. 487.01(1)(*b*) is concerned, take, as just one example, the fact that the availability of a Part VI authorization is limited to certain offences included under the definition of "offence" in s. 183. Should the police seek authorization for a search concerning an offence not included within that definition, though the "no other provision" test would be satisfied, it would fall to an analysis under subsection (1)(*b*) to guard against the issuance of a warrant that Parliament obviously anticipated and deliberately excluded: S. Coughlan, "*R. v. Ha*: Upholding General Warrants without Asking the Right Questions" (2009), 65 C.R. (6th) 41, at pp. 41-43.

[99] Leaving that aside, my colleague provides no guidance as to the type of conduct that he would classify as abusive, even as he stresses that "judges asked to issue general warrants must be vigilant to ensure that the right to be free against unreasonable searches and seizures is fully given effect" (para. 189). Presumably, he would leave it to individual judges to decide the matter on a case-by-case basis under s. 487.01(1)(*b*), thereby accepting his own form of uncertainty in the process. As I have acknowledged, the substantive approach to which I ascribe is not airtight — but it is no more porous than the total reliance on the "best interests" test that my colleague endorses.

[100] I turn then to my colleague's second concern — that I have impermissibly read investigative necessity, a concept peculiar to Part VI, into s. 487.01. With respect, my approach to s. 487.01(1)(*c*) has nothing to do with investigative necessity.

[101] The requirement under s. 186(1)(*b*) that a Part VI authorization be necessary is concerned with a *factual* question. In requiring that other procedures "have been tried and have failed", or that they were "unlikely to succeed", or that the "urgency of the matter is such that it would be impractical" to use them, it is apparent that s. 186(1)(*b*) is concerned with whether the factual circumstances of a particular case necessitate the use of the powers granted under Part VI. LeBel J. explained as much for the Court in *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992:

> Parliament and the courts have indeed recognized that the interception of private communications is a serious matter, to be considered only for the investigation of serious offences, in the presence of probable grounds, and with a serious testing of the need for electronic interception in the context of the particular investigation and its objects . . . . There must be, practically speaking, no other reasonable alternative method of investigation, in the circumstances of the particular criminal inquiry. [Emphasis added; emphasis in original deleted; para. 29.]

[102] By contrast, the "no other provision" test asks a *legal* question. The inquiry is not whether alternative search techniques have been exhausted, or whether they are unlikely to work, or whether there is urgency in the circumstances. Rather, the question is whether the purportedly "new" investigative technique is actually or substantively equivalent to a technique that is already authorized by law. In other words, under the "no other provision" test, the police are not asked to show why an

alternative authorization *would not work* on the facts of a particular case, but rather why it is *substantively different* from what Parliament has already provided. Though the fact that an alternative authorization will satisfy the investigative objective of the police may be helpful as a factor in demonstrating its substantive equivalence, the inquiry under the "no other provision" test remains focused on the latter point, not the former. If the police successfully make this showing, the inquiry under s. 487.01(1)(*c*) ends.

[103] Two final matters raised by Justice Cromwell's reasons warrant clarification.

[104] First, I do not conclude — nor should I be taken as suggesting — that the police acted duplicitously or in bad faith in seeking the general warrant in the case at hand. There is no evidence to that effect and I have no reason to believe that the police acted other than in good faith. Put simply, we do not know what motivated the police, nor is that the real issue. Ultimately, whether the police could or could not obtain a Part VI authorization in this case is irrelevant insofar as the "no other provision" requirement is concerned. What does matter is that we have been provided with nothing that would assist the police in meeting their burden to show that the impugned technique was *substantively different* from an intercept.

[105] Second, the approach I endorse does not take investigative flexibility off the table. As *Ha* and *Brand* make clear, it is a factor that a judge may consider in deciding whether an investigative technique is substantively different such that a

general warrant should issue. But it is not the only factor, and it must be approached with caution, particularly in cases like the present one, where the issuance of a general warrant may be a convenient way for the police to avoid the rigours of another search provision that is substantively equivalent.

IV. Conclusion

[106] For these reasons, I am of the view that the approach taken by the police in this case cannot be sanctioned. The general warrant is invalid because the investigative technique it authorized was substantively equivalent to an intercept. On the facts here, the general warrant served only to provide a means to avoid the rigours of Part VI. As the Crown recognized, the police could have sought a Part VI authorization. It is enough to decide this appeal to conclude that they should have.

[107] That said, though we are not presented with such a scenario, I would not go so far as to conclude that a general warrant can *never* prospectively authorize the delivery of future private communications to the police on a continual basis over a sustained period of time. If an issuing judge is satisfied that a particular investigative technique is substantively different such that the provisions of Part VI, or of any other statute, do not provide for the search, it would be open to the judge to issue the warrant, assuming other requirements are satisfied. The judge must, of course, conclude that the warrant is in the "best interests of the administration of justice" (s. 487.01(1)(*b*)) and the judge "shall" impose such terms and conditions as necessary to ensure that the search is reasonable in the circumstances (s. 487.01(3)).

[108] I would allow the appeal and quash the general warrant and related assistance order.

The reasons of McLachlin C.J. and Cromwell J. were delivered by

CROMWELL J. —

I. Overview

[109] TELUS Communications Company ("Telus") stores in its databases a copy of all text messages sent by or to its subscribers. The main question on this appeal is whether, when the police wished to obtain copies of these stored messages, they required a wiretap authorization. My colleagues Abella J. and Moldaver J. would hold that they did, although for markedly different reasons. I respectfully disagree. Like the Ontario Superior Court judge whose decision is under appeal, my view is that a wiretap authorization was not required. I would therefore dismiss the appeal.

II. Facts, Proceedings and Issues

[110] We are concerned in this case with particular investigative techniques that may be authorized under the *Criminal Code*, R.S.C. 1985, c. C-46, in the context of the police wishing to have lawful access to the content of text messages. Before turning to an analysis of the specific legal issues we confront, I will set out some

technical background about text messaging and the range of investigative techniques that may be open to the police to gain access to them. I will then set out a brief account of the proceedings which bring the case to us and the specific issues that we must resolve.

A. *Telus's Text Messaging Service*

[111] Text messaging, technically known as Short Message Service ("SMS"), is a communication service using standardized communications protocols and mobile telephone service networks to allow for the exchange of short text messages from one mobile phone to another.

[112] Telus's system of text message delivery is the same as that of other telecommunications service providers. When a message is sent by a Telus subscriber, it is transmitted to a Telus cell tower and then routed to a Mobile Switching Centre ("MSC") which is the computerized mainframe to the Telus network. Within the MSC is Telus's Short Message Service Centre ("SMSC"), which uses routing engines to attempt to deliver the message to its destination. If the recipient is also a Telus subscriber, the message will then be sent from Telus's SMSC to a cell tower which will forward the message to the recipient's phone. If the recipient is not a Telus subscriber, the message will pass from Telus's SMSC to the SMSC of the recipient's provider and then through a cell tower to the recipient's phone. Where the destination phone is not available (for example, because it is turned off or does not have service reception) the text message remains in the Telus SMSC for up to five days. If the

recipient phone does not become available within that timeframe, the message is deleted. The sender is not informed if a message is not delivered.

[113] Telus differs from most other providers in that it makes electronic copies of the text messages that pass through its system and stores those copies in one of four computer databases for at least 30 days. There are three PSMS databases (namely, PSMS 1 (primary database), PSMS 2 (secondary database), and PSMS 3 (tertiary database)), which receive messages within up to approximately 15 minutes of the time they are sent. Which PSMS a message goes to depends on the capacity of each database. All text messages received by a Telus customer are copied, and the copy is forwarded to the databases when the Telus subscriber's phone receives the message from the Telus SMSC. When a Telus subscriber sends a text message, it is copied when it arrives at the Telus SMSC and the copy is stored in a database. Telus also maintains a fourth database, named PECSMS, which receives messages between 2 to 8 hours after they are sent. At the time this case was heard at first instance, Telus expected that by April 2011, PECSMS would be the sole repository for all text message content; it would cease to use the PSMS databases.

[114] Telus copies text messages in order to facilitate troubleshooting and dealing with customer complaints. As I will explain, Telus in doing this is intercepting the messages and it has legal authority under the *Code* to do so without a wiretap authorization. In my view, Telus's stated purpose, coupled with the fact that most other service providers in Ontario transmit text messages without storing copies

of them in this manner, makes it clear that this additional step is not part of the communications process. Unlike e-mail messages, which must go through transient storage as they are transmitted, storage of the type in issue here is not inherent to the communication of text messages.

B. *Text Messages and Investigative Techniques*

[115] The *Code* provides at least three potential ways for the police to obtain authorization to acquire the content of stored text messages from Telus: a production order, a general warrant and a so-called "wiretap" interception authorization. The police in this case sought and obtained a general warrant as a sort of enhanced production order, but Telus's contention is that they were required to seek a wiretap authorization. It will be helpful to describe these three investigative techniques briefly, because the requirements of each are somewhat interrelated.

1. Production Order

[116] The police may obtain the contents of stored text messages by means of a production order under s. 487.012. This provision allows a judge or justice to order a person "to produce documents, or copies of them . . . or to prepare a document based on documents or data already in existence and produce it" (s. 487.012(1)(*a*) and (*b*)). The conditions for issuing a production order are similar to those for a search warrant. The issuing justice or judge must be satisfied by information on oath that an offence has been or is suspected to have been committed, the documents or data will afford

evidence respecting the commission of the offence and that the person to whom the order is directed has possession or control of the documents or data (s. 487.012(3)). In addition, the person to whom the order is directed cannot be a person under investigation (s. 487.012(1)).

[117] When presented with a production order, Telus is required to produce to police, documents or data, or copies thereof, which it already has. In this way, police obtain copies of text messages that have already been sent or received by the subscribers and stored in Telus's databases. It has been assumed and I will accept for the purposes of this case that a production order cannot issue for documents or data not yet in existence (see ss. 487.012(1)(*b*) and 487.012(3)(*c*)).

[118] I would add that s. 487.012, on its face, allows a judge or justice to order production of text messages from a provider's databases through a series of daily authorizations. Section 487.012 sets relatively few limits on the issuance of production orders. Unlike the other authorizations that concern us here, it does not require a finding by the judge that the order is necessary to the police investigation, nor does it require that a production order be in the best interests of the administration of justice. Like the reviewing judge, I accept that the police could have accessed the text messages stored in Telus's databases pursuant to such a series of orders.

2. General Warrant

[119] A judge may issue a general warrant, provided for in s. 487.01, to authorize a peace officer to "use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure" (s. 487.01). The issuing judge must be satisfied on the basis of information on oath that there are reasonable grounds to believe that an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique for which the police seek authorization.

[120] Given the wide array of techniques that may be authorized under a general warrant, Parliament has imposed additional, stringent conditions. First, unlike search warrants and production orders that may be issued by judges or justices of the peace, general warrants may only be issued by judges (s. 487.01(1)). Second, "the judge [must be] satisfied that it is in the best interests of the administration of justice to issue the warrant" (s. 487.01(1)(*b*)). Third, a general warrant must "contain such terms and conditions as the judge considers advisable to ensure that the search or seizure authorized by the warrant is reasonable in the circumstances" (s. 487.01(3)). Fourth, a general warrant may be issued only if "there is no other provision . . . that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done" (s. 487.01(1)(*c*)). In other words, a general warrant may not be used to authorize a "technique, procedure or device to be used or . . . thing to be done" if there are other provisions in the *Code* (or elsewhere) that could authorize it. (I will refer to this as the "no other provision"

requirement.) Telus's position is that this requirement was not met because the wiretap provisions of the *Code* provide for authorization of the technique which the police wished to use.

3. Wiretap Authorization

[121] An authorization to intercept private communications under Part VI of the *Code* allows police to receive messages as they are being sent or received by subscribers. These sorts of authorizations are subject to even more strict conditions than those which apply to general warrants. They may only be issued by a judge of a superior court of criminal jurisdiction. The Attorney General, the Minister of Public Safety and Emergency Preparedness or a specially designated agent must bring the application (s. 185(1)). There are specific and detailed provisions relating to what must be placed before the judge. The issuing judge must be satisfied not only that it would be in the best interests of the administration of justice to issue the authorization but also that the so-called "investigative necessity" test has been met (s. 186(1)). This means that the judge must be satisfied 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" (s. 186(1)). The authorization may generally not be valid for more that 60 days (s. 186(4)(*e*)) and there are notice and reporting requirements (s. 196).

[122] Where a wiretap authorization has issued in relation to text messages, Telus installs a device which automatically re-routes a copy of each text message to a police wire room or listening post. When a text message is sent by a Telus subscriber, the device re-routes a copy of the message when it arrives at the Telus SMSC. When a text message is received by a Telus subscriber, the wiretap device re-routes the copy when the subscriber's phone receives the message. With an intercept authorization, then, police have access to messages "in real time" as they are being sent and received.

C. *Proceedings*

[123] The police sought and obtained a general warrant in this case. It directed Telus to provide them with copies of the stored text messages to and from two of its subscribers. The warrant required production of messages sent and received before it was issued and, as well, of messages sent and received roughly two weeks into the future. Only the authorization in relation to the future production is in issue here. For those future messages, Telus was required by 2:00 p.m. each day Tuesday to Friday, to provide copies of all messages that had been sent or received between 11:00 a.m. on the previous day and 11:00 a.m. that same morning. On Mondays, Telus had to provide by 2:00 p.m. copies of all messages that had been sent or received between 11:00 a.m. Friday and 11:00 a.m. Monday. In addition, the general warrant required Telus to provide the police with subscriber information for all of the telephone numbers which exchanged texts with the two subscribers in question. Thus, this

general warrant was similar to a production order in that it required the production of copies of stored messages and related subscriber information. But it was different from a production order in that it prospectively authorized the production of these copies.

[124] Telus applied to quash the general warrant and its application was mainly dismissed by Sproat J. (2011 ONSC 1143, 105 O.R. (3d) 411). Telus's principal ground for its challenge to the general warrant was that it authorized an interception, a technique that could be authorized under Part VI of the *Code*. It followed that a general warrant could not issue because the "no other provision" requirement for a general warrant was not met.

[125] The reviewing judge rejected this contention. He did not think that what the police were authorized to do under the general warrant was an interception. The police were asking for copies of the messages already stored in Telus's databases; they were not asking permission to "intercept private communications". In his view, the word "intercept" requires a real time capture of otherwise transient communications, and this does not cover obtaining copies of messages stored in a database. The wiretap provisions could only be used to authorize interceptions and therefore would not apply to the investigative technique used by the police in this case. It followed, in the reviewing judge's opinion, that a general warrant could issue.

[126] Telus also advanced a number of other arguments which were rejected by the reviewing judge. Telus submitted that police should have waited until the end of the 14-day period covered by the general warrant and applied for a single production order. The judge rejected Telus's submission that police had to wait so long to obtain the messages. He also found that while police could have gone to the Justice of the Peace to obtain 14 separate production orders, that would have been an impractical solution in the circumstances (para. 76). He identified various drawbacks of requiring police to seek 14 authorizations including the need to make repeated, daily applications potentially involving different judicial officers and the inconvenience to Telus resulting from having to deal with daily warrants requiring prompt response (para. 70). Sproat J. concluded that a single general warrant that authorized police to receive deliveries of messages by e-mail over roughly two weeks was appropriate because "it would have been impractical for the police to obtain a daily warrant to achieve the investigative objective of obtaining stored text messages for daily review" (para. 76).

[127] The reviewing judge also dismissed Telus's submission that issuing a general warrant was not in the best interests of the administration of justice (s. 487.01(1)(*b*)). He held that the technique sought to be authorized was not an interception. The judge concluded that "it is not open to the court to decide on public policy grounds that the legislative scheme is inappropriate and, under the guise of what is in the best interests of the administration of justice, effectively expand the ambit of Part VI of the *Criminal Code*" (para. 80). The reviewing judge similarly

rejected Telus's submissions that the general warrant was unwieldy and unworkable and imposed an undue burden. The judge noted that similar concerns had been dismissed by this Court in *Tele-Mobile Co. v. Ontario*, 2008 SCC 12, [2008] 1 S.C.R. 305, at para. 60.

D. *Issues*

[128] The principal point advanced by Telus on appeal is that the investigative technique authorized by the general warrant was, in fact, an interception of a private communication and therefore, by virtue of the "no other provision" requirement in s. 487.01(1)(*c*), could only be authorized under Part VI of the *Code*. My colleague Abella J. agrees with this position while I, respectfully, do not. My colleague Moldaver J., on the other hand, does not find it necessary to address Telus's principal submission. Instead, he would hold that even if the general warrant is not, strictly speaking, an interception, it authorizes a technique that is substantively the same as an interception and therefore should be excluded from authorization by a general warrant by virtue of the "no other provision" requirement in s. 487.01(1)(*c*). Thus there are two issues:

1. Is the investigative technique authorized by the general warrant in this case an interception which requires an authorization under Part VI of the *Code*?

2. If the seizure of the stored text messages is not an interception, is the issuance of a general warrant nevertheless barred by the "no other provision"

requirement in s. 487.01(1)(*c*) because the technique sought to be authorized was substantively the equivalent of a wiretap?

III. Analysis

A. *First Issue: Is the Investigative Technique Authorized by the General warrant in this Case an Interception Which Requires An Authorization Under Part VI of the Code?*

[129] Telus submits that a general warrant could not issue in this case because the technique for which police were seeking authorization was the interception of private communications. The investigative technique of interception of private communications can be authorized by a judge under s. 186 in Part VI of the *Code*. Therefore, goes the argument, a general warrant should not have been issued because the police did not meet the "no other provision" requirement for a general warrant (s. 487.01(1)(*c*)).

[130] My colleague Abella J. substantially accepts this position. She would hold that the general warrant purported to authorize an interception because it allowed for "the *prospective* production of future text messages from a service provider's computer" (para. 15 (emphasis in original)). I understand "the *prospective* production of future text messages" to mean that at the time the warrant issues, at least some of the messages that are required to be disclosed have not yet come into existence. In my respectful view, this general warrant did not authorize an interception.

[131] The investigative technique authorized by the general warrant in this case was not an interception of private communications that could be authorized by s. 186. The general warrant provides the police with copies from Telus of stored messages which it had previously intercepted; police only obtain disclosure of the messages when Telus compiles them from its databases and sends them by e-mail. Far from being a "technical" difference, the distinction between disclosure of an intercepted communication and interception of a communication is fundamental to both the purpose and the scheme of the wiretap provisions.

1. The Text, Context and Scheme of Part VI

[132] The question of whether what the police did under this general warrant is an interception of a private communication is one of statutory interpretation. In my view, when we read the text of the statutory provisions in its full context, it is clear that the general warrant does not authorize an interception that requires a Part VI authorization.

[133] As a general rule, the police require an authorization to intercept private communications by means of any electro-magnetic, acoustic, mechanical or other device. The key words are thus "intercept" and "private communication".

[134] The word "intercept" is given a non-exhaustive definition: it includes "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof" (s. 183). The definition of the term "private communication" is

linked to the concept of interception. Stripping the definition of "private communication" down to its essentials, a private communication is a communication 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" (s. 183).

[135] There is no doubt that the text message is a private communication. As we shall see, there is also no doubt that text messages were intercepted by Telus by means of an electro-magnetic, acoustic, mechanical or other device. The question is whether the police also intercepted those messages when Telus turned over to them copies of sent and received messages previously intercepted by Telus and stored in its databases.

[136] This brings me to a fuller examination of the purpose, text and scheme of the wiretap provisions. In my view, this analysis sheds the most light on Parliament's intent as to whether the technique adopted by the police in this case constitutes an interception. The relevant provisions are set out in the Appendix.

[137] Fundamental to both the purpose and to the scheme of the provisions is the distinction between *the interception* of private communications and *the disclosure, use or retention* of private communications that have been intercepted. The purpose, text and scheme of Part VI show that the disclosure, use or retention of intercepted private communications is distinct from the act of interception itself.

[138] When the original wiretap provisions were introduced in 1973, the explanatory note to the Bill outlined that one of its purposes was to create three distinct types of offences. Two are relevant to this case. The first offence relates to the *interception* of private communications by the use of any electro-magnetic, acoustic, mechanical or other device. The second relates to the *disclosure* of private communications intercepted by the use of any such device (Explanatory Note, Bill C-176, *Protection of Privacy Act*, 1st Sess., 29th Parl. (S.C. 1973-74, c. 50). While explanatory notes are less authoritative than legislated statements of purpose, they nonetheless provide some insight to legislative purpose: R. Sullivan, *Sullivan on the Construction of Statutes* (5th ed. 2008), at p. 272. The explanatory note thus shows that from its inception, one of the purposes of the legislation was to distinguish between interceptions of private communications and the subsequent and separate acts of disclosure or use of intercepted private communications. This shows that Parliament understood interception and disclosure of intercepted communications to be different things and therefore did not intend to include disclosure or use of intercepted communications as part of the concept of interception.

[139] An early commentator on the legislation noticed that this distinction was fundamental to the statutory scheme. David Watt (now Watt J.A.) considered whether or not replaying, rehearing, or re-recording a previously recorded conversation constituted an "interception" and concluded:

> Each replaying or rehearing of the original interception may well constitute a use or disclosure of the intercepted communication within the

> relevant prohibition but, use or disclosure is not, perforce, interception, and to equate the two is to ignore the fundamental statutory distinction between them.
>
> *Law of Electronic Surveillance in Canada* (1979), at p. 44. [Emphasis added.]

[140] This distinction between interception and disclosure is reflected in the structure of the offence-creating provisions in Part VI. In other words, the text of the legislation precisely reflects the purpose set out in the Explanatory Note. Part VI creates distinct offences reflecting the purpose set out in the Explanatory Note.

[141] One offence, as noted, prohibits the *interception of a private communication*. Section 184 of the *Code* provides that "[e]very one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years". There are a number of exceptions which I will review shortly. The other offence is concerned with *disclosure or use of intercepted information*. Section 193 of the *Code* provides that it is an indictable offence to use or disclose the content or existence of an intercepted communication without the consent of the originator or the person intended to receive it. Once again, there are several exceptions which I will return to in a moment. The enactment of these two distinct offences underlines that the act of interception and the act of disclosure or use of intercepted communications are distinct acts which receive distinct treatment under the statutory scheme.

[142] Turning to the first offence which deals with interceptions, there are several "saving provisions" that exclude certain acts that would otherwise constitute illegal interceptions. These exclusions from liability are relevant to understanding the statutory scheme because they distinguish *interception* of communications from *use or retention* of intercepted communications. It is not necessary to go into all of the details, but the exemptions from criminal liability fall into three categories. It is not an offence to intercept a private communication by means of an electro-magnetic, acoustic, mechanical or other device if (i) the interception occurs with consent (s. 184(2)(*a*)); (ii) the interception is authorized in accordance with the authorization provisions (s. 184(2)(*b*)); or (iii) the interception is done for the purposes of providing a communications service or by a servant of Her Majesty engaged in radio frequency spectrum management, or for the purposes of managing or protecting a computer system, (s. 184(2)(*c*), (*d*) and (*e*)).

[143] The important point is that the third of these saving provisions — the one in relation to computer system interceptions — makes a distinction between *interception* on the one hand and *use* or *retention* of the intercepted communications on the other. Section 184(2)(*e*) excludes from the offence the interception of a private communication passing through a computer system by a person in control of it, provided that the interception is reasonably necessary for managing the quality of service or protecting the computer system. This exception is qualified by s. 184(3) which relies on the distinction between *interception* and *use or retention*. Under s. 184(3), a private communication *intercepted* by a person in control of a computer

system may only be *used or retained* if it is essential to prevent harm to the system or if it is disclosed as provided for elsewhere in the legislation.

[144] Thus, within the interception offence provisions, there is a distinction made between interceptions and the use or retention of intercepted communications. This suggests that Parliament viewed those acts as different and distinct.

[145] That brings us to the second offence in the scheme, the offence prohibiting the use or disclosure of previously intercepted private communications. Under s. 193(1), it is an offence to *use* or *disclose* the content or existence of a private communication that has been intercepted without consent. Note that the use and disclosure offence relates to a "private communication or any part thereof or the substance, meaning or purport thereof". The existence of this offence as something distinct from the interception offence shows that Parliament treated interception and disclosure or use as distinct concepts.

[146] A comparison of the exemptions in ss. 184 and 193 reinforces my position. The exemptions in s. 193 are far more permissive than those in s. 184, especially with respect to criminal investigations. Under s. 184, police can only intercept communications if they are authorized to do so (s. 184(2)(*b*)) or in certain exceptional circumstances (s. 184.4). By contrast, s. 193 includes broad exemptions that permit disclosure of intercepted communications in a range of circumstances including in the course of civil or criminal proceedings (s. 193(2)(*a*)), and "in the course of or for the purpose of any criminal investigation" (s. 193(2)(*b*)). Had

Parliament understood disclosure of intercepted private communications to be a form of interception, one would expect substantial correspondence between the exemptions relating to interception and those relating to disclosure. This is plainly not the case.

[147] This point is even further supported by a comparison of the particular exemptions that apply to communication service providers, set out in ss. 193(2) and 184(2). Recall that providers of communication services are exempt from the interception offence when they intercept communications for the purposes of service delivery (s. 184(2)(*c*)). There is a comparable exemption for service providers in relation to the disclosure offence. Section 193(2)(*d*) exempts from criminal liability disclosures in the course of the operation of a communications or computer system, provided that the disclosure is necessarily incidental to the purposes which provide such operators with an exemption from the interception offence. Thus, operators of communications systems such as Telus are exempted in certain circumstances from both the interception offence and the disclosure offence. This further underlines that Parliament viewed these activities as distinct.

[148] To sum up, the legislative scheme creates two distinct offences, one which deals with interception and the other with use or disclosure of a communication. Fundamental to the scheme is the distinction between these activities: if disclosure or use of a private communication were an interception of it, there would be no need to create the distinct disclosure or use offence. Similarly, the

exemptions from criminal liability show that Parliament distinguished between interception on one hand and retention, use and disclosure on the other.

2. Did the General Warrant Authorize an Interception of a Private Communication?

[149] How does this relate to what Telus and the police were doing under the general warrant in this case? To begin with Telus, no one disputes that it was intercepting text messages when it copied them for its own systems administration purposes. Similarly, it is agreed (and I will accept for the purposes of this appeal) that Telus did not commit the offence of unlawful interception. It performed interceptions for a permitted purpose which was exempted from criminal liability. Section 184(2)(*c*) makes it clear that it is not an offence for communication service providers such as Telus to intercept private communications where that is necessary for, among other things, quality control purposes. Under s. 193(2)(*d*), they also, for the same purposes, can disclose the intercepted communications without incurring criminal liability. There is, therefore, no question for the purposes of this appeal that Telus lawfully intercepted private communications.

[150] What about the actions of the police under the general warrant? They sought disclosure from Telus of information that it had already lawfully intercepted. The general warrant did not require Telus to intercept communications, but to provide copies of communications that it had previously intercepted for its own lawful purposes. There is no suggestion that Telus was carrying out these interceptions at the bidding of the police; interceptions carried out for police purposes would clearly

require authorizations as they would not fall within the exempt purposes under s. 184(2)(*c*). However, as the scheme of the legislation makes clear, disclosure or use of a lawfully intercepted communication is not an interception. As discussed in detail earlier, Part VI of the *Code* makes a fundamental distinction between, on one hand, *intercepting* — i.e. listening to, recording or acquiring a communication or the substance, meaning or purport thereof — and, on the other, *using or disclosing* a private communication or the substance, meaning or purport thereof or disclosing the existence of the communication. This distinction is recognized by the purposes of the provisions, by the creation of distinct offences for unlawful interception and unlawful use or disclosure and by the saving provisions which apply to the interception and disclosure offences.

[151] In my view, it is inconsistent with the fundamental distinction made by the legislation to conclude that the police were intercepting private communications when Telus provided them with copies of previously intercepted and stored text messages.

3. Abella J.'s Reasons

[152] That brings me to Abella J.'s reasons. She would hold that the general warrant purported to authorize an interception because it allowed for "the *prospective* production of future text messages from a service provider's computer" (para. 15 (emphasis in original)); the fact that the messages were stored in a database is simply a "technical" difference in Telus's service delivery system that should not "deprive

Telus subscribers of the protection of the *Code*": para. 3. Therefore, a wiretap authorization, not a general warrant, was required. This interpretation relies on the fact that the word "intercept" is defined to include "acquire a communication or . . . the substance, meaning or purport thereof" (s. 183) and the fact that wiretap authorizations are prospective in nature. I do not find this approach convincing for three reasons.

[153] My first difficulty is that Abella J.'s approach does not give effect to the clear distinction in the statute between interception and disclosure. For reasons I set out earlier, this distinction cannot in my view be dismissed as a mere "technical difference". The distinction is fundamental to the scheme of the provisions. Parliament treated "interception" and "disclosure" as separate acts, giving rise to different offences and different exemptions, even though they may relate to the same private communications. When Telus turns over to the police the copies of the communications that it has previously intercepted, Telus is disclosing the communications, not intercepting them again. I do not understand how this disclosure by Telus from its databases can be an interception by the police.

[154] The second difficulty with my colleague's position relates to her reliance on the definition of "intercept" in s. 183 and particularly on the fact that "intercept" includes "acquire the substance, meaning or purport" of a private communication. Read broadly, this definition of "intercept" means that any time the police acquire the content of a private communication by means of any electro-magnetic, acoustic,

mechanical or other device, they have engaged in an interception. In my view, the context and purpose of Part VI require the phrase "acquire the substance, meaning or purport" of a private communication to be read more narrowly.

[155] To begin, "acquire" must be understood in the context of the text surrounding it; it is found in a list that includes "listen to" and "record", both activities that occur simultaneously with the communication being intercepted. It is also used to explain the word "intercept" and I think it is clear that there are many ways to acquire the content of a communication that could not be thought of as an interception. 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, at para. 73; *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241, at para. 33; *R. v. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. v. Cross*, 2007 Can LII 64141 (Ont. S.C.J.), at paras. 25-27; *R. v. Little*, 2009 CanLII 41212 (Ont. S.C.J.), at para. 154; *R. v. Tse*, 2008 BCSC 906, [2008] B.C.J. No. 1766 (QL), at para. 198; *R. v. Weir*, 2001 ABCA 181, 281 A.R. 333, 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.

[156] As I see it, such a broad reading of "acquire" is inappropriate, given the scheme and purpose of the wiretap provisions. I will not repeat the analysis set out above. It flows from that analysis, however, that acquiring the content of a previously intercepted and stored communication cannot be an interception because that broad reading is inconsistent with the clear distinction between interception and disclosure in the provisions. Applied broadly, this interpretation of "acquire" would extend the scope of investigative techniques which require wiretap authorizations far beyond anything ever previously contemplated.

[157] That brings me to the temporal aspect of interception that Abella J. introduces, which is the third difficulty I see with her approach. As I understand it, the acquisition of the content of a private communication is an interception if the

acquisition is authorized prospectively. It follows that whether or not an act constitutes an interception depends not on the nature or timing of the act itself, but on when the act is authorized. It necessarily follows that the seizure of previously intercepted and stored text messages would not be an interception as long as it was authorized *after* the messages were stored. The police could obtain a production order at the end of every day during the period covered by the general warrant and there would be no interception. However, under this prospective authorization test, if the police were to seize the exact same information, in the same form and by the same means pursuant to an authorization issued *before* the messages were stored, they would be engaging in an interception. This approach seems to me to confuse the act of interception with the nature of its authorization.

[158] Interception is a technique, a way of acquiring the substance of a private communication. I do not understand how it could be that exactly the same technique, which acquires information in exactly the same form may be either a seizure of stored material or an interception, depending on the point in time at which the technique is authorized. But that is the result of my colleague Abella J.'s analysis. I cannot accept this conclusion.

4. Conclusion on the First Issue

[159] In my view, the investigative technique which the police were authorized to use by the general warrant was not an interception within the meaning of the wiretap provisions of the *Code*.

B. *Second Issue: If the Seizure of the Stored Text Messages Is not an Interception, Is the Issuance of a General Warrant Nevertheless Barred by the "no other provision" Requirement in Section 487.01(1)(c) Because the Technique Sought To Be Authorized Was Substantively the Equivalent of a Wiretap?*

[160] My colleague Moldaver J., like Abella J., would set aside the general warrant because the police did not meet the "no other provision" requirement in s. 487.01(1)(*c*). However, Moldaver J. reaches this conclusion by a different route which, as I understand it, relies on three main points. First, the general warrant is one of limited resort that should be used sparingly (para. 56). I respectfully do not accept this general proposition or the result to which its adoption leads in this case. Second, the technique proposed by police in this case is "substantively" the same as an interception and therefore cannot be authorized under s. 487.01(1) because of the "no other provision" requirement in para. (*c*). Respectfully, as I see it, the "substantive equivalency" test is not part of the analysis under s. 487.01(1)(*c*) and would not apply on the facts of this case even if it were. Third, given this "substantive" similarity, police resort to the general warrant amounts to a "misuse" of s. 487.01, a "convenient way" for police to avoid the rigours of wiretap authorizations. While I share my colleague's view that the courts should be vigilant for undue extension and abuse of the general warrant provisions, my respectful view is that this is an inappropriate case in which to give effect to those concerns.

1. <u>The Purpose of the General Warrant Provision</u>

[161] Moldaver J. counsels against literal interpretation of the provisions and espouses a purposive one. Of course, I agree that all legislation must be interpreted purposively. I respectfully part company about what results from a purposive interpretation of this provision.

[162] I begin with the purposes of the general warrant provision. I do not accept that the purpose of s. 487.01(1) is to provide authorizations only in very limited circumstances and that it therefore must only be used "sparingly". On the contrary, as numerous authorities have acknowledged, the provision is cast in wide terms. As one leading commentator put it:

> Through s. 487.01 (and s. 487.02), Parliament has provided a broad, plenary warrant-granting power intended to ensure that judicial authorization is legally available for virtually any investigative technique that can be brought within the *Hunter* conditions for judicial pre-authorization.
>
> (S.C. Hutchison, *Hutchison's Canadian Search Warrant Manual 2005* (2005), at p. 143)

When the Ontario Court of Appeal considered this issue in *R. v. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, at para. 35, leave to appeal refused, [2009] 3 S.C.R. vii, it rejected a restrictive interpretation of s. 487.01. Rather, the court affirmed the remedial character of s. 487.01 and cited its previous holding in *R. v. Lauda* (1998), 37 O.R. (3d) 513, at pp. 522-23, aff'd [1998] 2 S.C.R. 683, to the effect that the general warrant provides for a flexible range of investigative procedures; see also *R. v. Noseworthy* (1997), 33 O.R. (3d) 641, at p. 644.

[163] Taking into account this understanding of the purpose of s. 487.01, I approach the interpretation of the provision differently than my colleague. In particular, I do not accept as an imperative that s. 487.01 must be interpreted with a view to heavily restricting its use. The focus of the inquiry is on two matters (in addition of course to reasonable grounds to believe that an offence has been committed and that information concerning the offence will be obtained): is authorization for the "technique, procedure or device to be used or the thing to be done" provided for in any other federal statute and is it in the best interests of the administration of justice to authorize it to be done?

[164] Turning from the purpose of s. 487.01 to the text and purpose of s. 487.01(1)(*c*) specifically, its focus is on the *means* by which an investigation is carried out, not its *objective*. Section 487.01(1)(*c*) provides that a general warrant may issue if "there is no other provision . . . that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done". The words "technique", "procedure", "device to be used" and "thing to be done" all are concerned with *what* the police want to do, not *why* they want to do it. This paragraph does not require issuing judges to consider whether other techniques are similar or allow access to the same evidence; it simply asks if the *same technique* can be authorized by another provision.

[165] The jurisprudence under this provision has consistently taken this approach. MacPherson J.A. made this point in *Ha* when he observed, at para. 43, that:

> [t]he focus in the s. 487.01(1)(*c*) analysis is not on whether there are other investigative techniques that might accomplish the purported investigative purposes or goals of the police; rather the focus is on the particular investigative technique or procedure that the police seek to utilize and whether it can properly be authorized by another provision. [Emphasis added.]

This is not simply a narrow, literal interpretation of s. 487.01. Rather, it is an interpretation that reflects its purpose of conferring a broad judicial discretion to authorize the police to "use any device or investigative technique or procedure or do any thing", provided of course that the judge is satisfied that it is in the best interests of the administration of justice to do so, having due regard to the importance of the constitutional right to be free of unreasonable searches and seizures. I completely agree with MacPherson J.A., writing for the Ontario Court of Appeal in *Ha*, when he said that he saw "no policy reason for struggling to constrain the scope of s. 487.01 by adding words that were not expressly included by Parliament in the provision" (para. 37).

[166] I note that Moldaver J. relies on this same paragraph in *Ha* to support the view that investigative goals are to be taken into account in the s. 487.01(1)(*c*) analysis, suggesting that in this passage MacPherson J.A. adopted an approach which considered "substantive" differences between various techniques (para. 70). Read in

full, however, MacPherson J.A.'s reasons do not support that proposition. As I see it, MacPherson J.A. was not "[e]xplaining why the search sanctioned . . . in *Ha* was . . . substantively different from one involving multiple conventional warrants" (Moldaver J., at para. 70). This is clear not only in the portions of the paragraph which I cite above, but also from the way MacPherson J.A. summarizes his conclusion, at para. 41: "The simple fact is that there is no provision . . . that would authorize an unlimited number of covert entries and searches on private property over a two-month period." In performing the s. 487.01(1)(*c*) analysis, MacPherson J.A. simply compared the search for which the police sought authorization under a general warrant with other search provisions and concluded that none of them would permit authorization of what the police sought to do.

[167] Similarly, in *R. v. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. v. Ford*), at para. 50, Frankel J.A. for the court stated that "[r]esort to a general warrant is only precluded when judicial approval for the proposed 'technique, procedure or device or the doing of the thing' is available under some other federal statutory provision." There is no hint in his reasons that there is any substantive equivalency or investigative necessity analysis required.

[168] I am reinforced in my reading of s. 487.01(1)(*c*) by a comparison of that paragraph with s. 186(1)(*b*) which sets out the investigative necessity requirement that must be met before a wiretap can be issued. According to s. 186(1)(*b*) an authorization under that section cannot be given unless the judge is satisfied

> (*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.

In *R. v. Araujo*, 2000 SCC 65, [2000] 2 SCR 992, the Court established that, under s. 186(1)(*b*), a judge cannot issue an intercept authorization unless she is satisfied that "practically speaking" there is "no other reasonable alternative method of investigation in the circumstances of the particular criminal inquiry" (para. 29 (emphasis deleted)). The standard set by Parliament here is high; it is not enough that an interception would be "more efficacious" than some other available technique, it must be *necessary* to the investigation (*Araujo*, at para. 39).

[169] By contrast, under s. 487.01(1)(*c*), a judge only needs to be satisfied that the proposed technique cannot be authorized by provisions in the *Code* or some other Act of Parliament. The judge does not, in addition, need to be satisfied that the novel technique is necessary to the investigation or that it is not the substantive equivalent of something that can be authorized elsewhere. Parliament knew how to direct an issuing judge or justice to consider whether other investigative techniques would achieve the investigative objective. It did so in s. 186(1)(*b*). It did not do so in s. 487.01(1)(*c*).

[170] Of course, this does not mean that the court should authorize anything the police seek to do simply because it is not authorized elsewhere. The judicial discretion to issue the warrant must give full effect to the protection of reasonable

expectations of privacy as set out in the abundant jurisprudence under s. 8 of the *Canadian Charter of Rights and Freedoms*. Judges should not exercise their discretion so as to permit the police to use the general warrant to evade the pre-authorization requirements that Parliament has imposed on certain investigative techniques. However, as I will explain, my view is that those concerns should be addressed directly and specifically under s. 487.01(1)(*b*) when they arise, not by reading in a limitation in s. 487.01(1)(*c*) that is not there.

[171] To sum up on this point, there is no support in the text or the purpose of s. 487.01(1)(*c*), or in the jurisprudence, for building into it a "substantive equivalency" test. The paragraph asks a simple question: Does federal legislation provide for "a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done"? Where this threshold is met, the judge is entitled to consider granting the requested authorization. The further question of whether the authorization *ought* to be granted is not the focus of this paragraph of the section. Rather, as I will explain, whether a general warrant ought to issue is properly considered under s. 487.01(1)(*b*), which asks whether authorizing the warrant would be in the best interests of the administration of justice. Not only, in my view, is this approach supported by the text, purpose and jurisprudence. The alternative proposed by Moldaver J. also creates unnecessary uncertainty and distracts the issuing judge from the question of whether the technique sought to be authorized is inconsistent with the right to be free from unreasonable searches and seizures.

[172] I turn first to my concern about uncertainty. In my view, predictability and clarity in the law are particularly important in the area of judicial pre-authorization of searches. Judicial pre-authorization is a cornerstone of the *Charter*'s protection against unreasonable searches and seizures. The primary objective of pre-authorization is not to identify unreasonable searches after the fact, but to ensure that unreasonable searches are not conducted. The requirements for pre-authorization should be as clear as possible to ensure that *Charter* rights are fully protected.

[173] Clarity also serves an important practical objective. Generally, and unlike in this case, challenges to judicial pre-authorization of searches are made after the fact at trial. If successful, the admissibility of the evidence obtained under the authorized search is put at risk. The police cannot undo, after the fact, that during their investigation, they relied on what is ultimately found to be a defective authorization. This makes it of great practical importance for the law to be clear to judges and justices who are asked to authorize searches and to police officers who seek authorization.

[174] The approach adopted by my colleague Moldaver J. in my view is seriously deficient in this regard. No guidance is provided as to when one investigative technique should be found to be substantively the same as another and when the differences are merely technical. As I will discuss in the next section of my reasons, this uncertainty is apparent from my colleague's application of the "substantive equivalency" test in this case.

[175] Moreover, my view is that adopting this approach to s. 487.01(1)(*c*) will not assist issuing judges in giving effect to the constitutional guarantee of freedom from unreasonable searches and seizures. That issue should be addressed directly under s. 487.01(1)(*b*), not through a vague, unnecessary and largely semantic exercise of comparing how much one technique may be like another. As I shall discuss, even when that question is addressed directly in this case, the arguments against issuing the general warrant are, in my respectful view, unconvincing.

2. The "Substantive Equivalency" of the Proposed Technique and an Interception

[176] Even if I were to accept (which I do not) that s. 487.01(1)(*c*) is concerned with the substantive equivalency of various investigative techniques, I would not find the technique sought to be authorized here to be the substantive equivalent of a wiretap authorization. According to my colleague Moldaver J., the general warrant in this case authorized a technique that was in substance an interception "because it *prospectively* authorizes police access to *future* private communications on a *continual* basis over a sustained period of time. . . . But for the 24-hour time delay, the investigative techniques were the same" (paras. 61 and 68 (emphasis in original))

[177] Respectfully, this assertion is not borne out by the facts or consistent with the law.

[178] Turning first to the facts, a wiretap authorization alone would not allow the police to obtain the information that Telus was required to provide under the general warrant. In fact, as the evidence from Telus shows, three separate authorizations would be required in order to provide the police with the means to access the information provided to them under the general warrant. As I explained above, when Telus responds to a wiretap authorization, it installs a device which re-routes in real time a copy of each text message sent to and from a particular number to the police. The general warrant in this case requires Telus to do more: it has to sort through its databases to deliver stored text messages and it also has to provide the relevant subscriber information relating to them.

[179] In her affidavit filed before the reviewing judge, Corinne McNish, a Telus Security Analyst, indicated that three different authorizations would be necessary to obtain the information required under the general warrant: an authorization under s. 492.2(1) for a dial number recorder; an authorization under s. 492.2(2) to obtain telephone records; and a Part VI authorization. I would add that, in order to make use of a Part VI authorization, police would have to secure a wire room or listening post to receive the messages as well as officers to process the incoming information, to deal with the information obtained from the dial number recorder and to sort through the telephone records.

[180] In light of Telus's own evidence, then, it seems to me to be quite a stretch to assert that the investigative techniques were substantively the same.

[181] Notwithstanding these clear and significant differences between the two techniques, my colleague relies heavily on two facts in concluding that the techniques were substantively the same: the fact that there was only a 24-hour time delay in the police gaining access to the information under the general warrant and that the general warrant authorized the turning over of the stored messages "prospectively". As I see it, the first fact is not correct and the second does not support the conclusion drawn from it.

[182] Turning first to the time delay, my colleague finds that the time delay between when the messages were sent and when they were to be received by police was short enough that their production would constitute the substantive equivalent of an interception. While Moldaver J. declines to identify the point at which the period of delay would render the proposed technique substantively different from an interception, he concludes that "the 24-hour gap here fell short of the mark": footnote 2. Respectfully, I cannot agree for two reasons.

[183] First, as the general warrant itself makes clear, some of the messages that police were to receive would be delayed by 72 hours, not 24. The productions ordered under the general warrant were to begin on March 30 and end on April 16. On Tuesday March 30, Telus was to produce information from March 18 to March 30, and the Crown concedes that this could have been obtained by a production order and therefore could not be the subject of a general warrant. Applied over the next two and a half weeks, the general warrant created two different time gaps, as I described

earlier. On Tuesday through Friday, Telus was required to provide by 2:00 p.m. each day the messages sent and received between 11:00 a.m. the previous day and 11:00 a.m. that day. However, on weekends, there was a longer "gap". By 2:00 p.m. on Mondays, Telus was required to provide the messages stored between 11:00 a.m. the previous Friday and 11:00 a.m. on Monday. Thus, for twelve days, production was daily. However, on weekends, or for six days covered by the general warrant, there was a longer "gap" of 72 hours. The question therefore arises whether that 72-hour delay also "fell short of the mark" and if not, whether police would need different authorizations for the messages they received on Mondays than they would for the messages they received on the other days of the week.

[184] Second, because I agree with the reviewing judge that police could have obtained a series of daily production orders, I have difficulty accepting that the 24-hour "gap" on which Moldaver J. relies makes the general warrant substantively equivalent to an interception. A series of daily production orders would have provided police with copies of the text messages within 24 hours of the time that they were sent. On my colleague's understanding of what is substantively an interception, then, some production orders could also be the equivalent of interceptions. This, as I see it, underlines the confusion and uncertainty inherent in the substantive equivalency approach to s. 487.01(1)(*c*).

[185] The second fact advanced in support of the finding of substantive equivalency is that the authorization is "prospective". As I pointed out earlier,

however, it is hard to understand how exactly the same technique either is or is not equivalent to an interception, depending on the point in time that it is authorized. If we accept for the purposes of this appeal, which I do, that the police could lawfully obtain daily production orders, I simply cannot understand how authorizing that technique two weeks earlier converts the production order into a wiretap authorization.

[186] Finally, the conclusion of substantive equivalency is inconsistent with the text and scheme of the wiretap provisions themselves. As I have explained at length earlier, the act of disclosure of previously intercepted private communication has been identified and treated in the *Code* as a separate and distinct act from that of interception itself. With respect, I cannot accept that what Parliament has made a legally significant distinction is merely a technical difference.

[187] To sum up, even if one were to accept reading into s. 487.01(1)(*c*) a "substantive equivalency" test, neither the facts nor the law would support its application in this case, in my respectful view.

[188] This also underlines, as I see it, the confusion and uncertainty that would flow from adopting such a test. My colleague provides no meaningful guidance on this point aside from a 24-hour "gap" guideline. The latter is problematic, however, because it conflicts with the availability of daily production orders under s. 487.012. In my view, issuing judges and police investigators should not be left to draw the line

on their own and then to hope, with little reason for optimism, that they will be found to have been right after a *voir dire* at a future trial.

3. Dealing with Abuses of General Warrants

[189] This brings us to the real heart of the matter: whether the general warrant should not have been issued because it represents, as my colleague would have it, a "misuse" of s. 487.01, an "easy way out", or a "convenient way", "device" or "hook", that allows the police to "escape the rigours" of Part VI (paras. 72, 81, 90 and 105). As I read Moldaver J.'s reasons, the proposed interpretation of s. 487.01(1)(*c*) is driven by a need to preclude abuses of the general warrant power. I accept that judges asked to issue general warrants must be vigilant to ensure that the right to be free against unreasonable searches and seizures is fully given effect by any investigative technique that is authorized. However, my view is that this analysis should be undertaken directly under s. 487.01(1)(*b*), not through the lens of asking the question of whether two techniques are substantively equivalent.

[190] As MacPherson J.A. wisely pointed out in *Ha*, the "no other provision" requirement in s. 487.01(1)(*c*) is not the only requirement that must be met before a general warrant may be issued (para. 44). The section should not be approached on the assumption that Parliament intended that every investigative technique not authorized elsewhere could be authorized under s. 487.01(1): see, for example, S. Coughlan, "*R. v. Ha*: Upholding General Warrants without Asking the Right Questions" (2009), 65 C.R. (6th) 41. Rather, the judge asked to issue the warrant

must also be satisfied that it is in the best interests of the administration of justice to authorize the particular technique (s. 487.01(1)(*b*)). This is the provision under which potential abuses of the general warrant should be addressed, in my view. Of course, even where the requirements in s. 487.01(1)(*b*) and (*c*) are met, s. 487.01(3) requires that a general warrant contain "such terms and conditions as the judge considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances".

[191] Section 487.01(1)(*b*) was not raised in this appeal and I do not want to say much about it beyond my view that it is the place in s. 487.01 that addresses concerns about whether a new investigative technique is one that should be authorized. That said, I do not find Moldaver J.'s concerns raised under the rubric of the proposed "substantive equivalency" test at all compelling.

[192] First, I would not conclude that police sought a general warrant in this case as a "convenient way" to avoid the rigours of Part VI. Of course, there is no evidence of that. Second, I do not agree with the claim that the privacy interests at stake in this case are exactly the same as those in issue where a wiretap authorization is sought. The reviewing judge accepted, and I agree, that warrants could issue daily to provide the police with copies of the stored messages. I fail to see how the affected privacy interests are different if permission to do that is granted two weeks in advance. Third, for all of the reasons identified by the reviewing judge, the general warrant was a more practical approach than a series of production orders. Fourth, the

general warrant authorized a technique that was not only different from an interception but was also more responsive to the needs of police. In particular, it significantly reduced the burden on the police in terms of resources to staff a wireroom and to extract information from subscriber records and dial number recorders. As I see it, the general warrant achieved the legitimate aims of the police investigation in a much more convenient and cost-effective manner than any other provision would have allowed.

[193] Of course, the general warrant had the effect of shifting costs to Telus. But that has nothing to do with the privacy interests of the subscribers. Moreover, Telus advanced evidence and argument in relation to the burden the general warrant placed on it, but those submissions were flatly rejected by the reviewing judge and not renewed in this Court.

[194] On the record before us, I do not see evidence of "misuse" of s. 487.01 or an attempt by police to "escape the rigours" of Part VI. What I see is effective and practical police investigation by a relatively small municipal police force which is fully respectful of the privacy interests of the targets of the investigation and other Telus subscribers.

C. *Conclusion*

[195] For these reasons, I find that the general warrant did not authorize an interception requiring a Part VI wiretap authorization and that the "no other provision" requirement of s. 487.01(1)(*c*) was met.

IV. Disposition

[196] I would dismiss the appeal.

APPENDIX

Criminal Code, R.S.C. 1985, c. C-46

PART VI

INVASION OF PRIVACY

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;

. . .

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.

(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).

(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).

. . .

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,

. . .

(*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.

. . .

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.

. . .

(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.

. . .

193. (1) Where a private communication has been intercepted by means of an electro-magnetic, acoustic, mechanical or other device without the consent, express or implied, of the originator thereof or of the person intended by the originator thereof to receive it, every one who, without the express consent of the originator thereof or of the person intended by the originator thereof to receive it, wilfully

(***a***) uses or discloses the private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof, or

(***b***) discloses the existence thereof,

is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

(2) Subsection (1) does not apply to a person who discloses a private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof or who discloses the existence of a private communication

(***a***) in the course of or for the purpose of giving evidence in any civil or criminal proceedings or in any other proceedings in which the person may be required to give evidence on oath;

(***b***) in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted;

(***c***) in giving notice under section 189 or furnishing further particulars pursuant to an order under section 190;

(***d***) in the course of the operation of

(i) a telephone, telegraph or other communication service to the public,

(ii) a department or an agency of the Government of Canada, or

(iii) services relating to the management or protection of a computer system, as defined in subsection 342.1(2),

if the disclosure is necessarily incidental to an interception described in paragraph 184(2)(***c***), (***d***) or (***e***);

(***e***) where disclosure is made to a peace officer or prosecutor in Canada or to a person or authority with responsibility in a foreign state for the investigation or prosecution of offences and is intended to be in the interests of the administration of justice in Canada or elsewhere; or

(***f***) where the disclosure is made to the Director of the Canadian Security Intelligence Service or to an employee of the Service for the purpose of enabling the Service to

perform its duties and functions under section 12 of the *Canadian Security Intelligence Service Act*.

. . .

PART XV

SPECIAL PROCEDURE AND POWERS

. . .

487. (1) A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(*a*) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

(*b*) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(*c*) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or

(*c.1*) any offence-related property,

may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(*d*) to search the building, receptacle or place for any such thing and to seize it, and

(*e*) subject to any other Act of Parliament, to, as soon as practicable, bring the thing seized before, or make a report in respect thereof to, the justice or some other justice for the same territorial division in accordance with section 489.1.

(2) If the building, receptacle or place is in another territorial division, the justice may issue the warrant with any modifications that the circumstances require, and it may be executed in the other territorial division after it has been endorsed, in Form 28, by a justice who has jurisdiction in that territorial division. The endorsement may be made on the original of the warrant or on a copy of the warrant transmitted by any means of telecommunication.

(2.1) A person authorized under this section to search a computer system in a building or place for data may

(*a*) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

(*b*) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

(*c*) seize the print-out or other output for examination or copying; and

(*d*) use or cause to be used any copying equipment at the place to make copies of the data.

. . .

487.01 (1) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property if

(*a*) the judge is satisfied by information on oath in writing that there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed and that information concerning the offence will be obtained through the use of the technique, procedure or device or the doing of the thing;

(*b*) the judge is satisfied that it is in the best interests of the administration of justice to issue the warrant; and

(*c*) there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done.

. . .

(3) A warrant issued under subsection (1) shall contain such terms and conditions as the judge considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances.

. . .

(5.1) A warrant issued under subsection (1) that authorizes a peace officer to enter and search a place covertly shall require, as part of the terms and conditions referred to in subsection (3), that notice of the entry and search be given within any time after the execution of the warrant that the judge considers reasonable in the circumstances.

. . .

487.012 (1) A justice or judge may order a person, other than a person under investigation for an offence referred to in paragraph (3)(*a*),

(*a*) to produce documents, or copies of them certified by affidavit to be true copies, or to produce data; or

(*b*) to prepare a document based on documents or data already in existence and produce

it.

(2) The order shall require the documents or data to be produced within the time, at the place and in the form specified and given

(*a*) to a peace officer named in the order; or

(*b*) to a public officer named in the order, who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

(3) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to believe that

(*a*) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;

(*b*) the documents or data will afford evidence respecting the commission of the offence; and

(*c*) the person who is subject to the order has possession or control of the documents or data.

(4) The order may contain any terms and conditions that the justice or judge considers advisable in the circumstances, including terms and conditions to protect a privileged communication between a lawyer and their client or, in the province of Quebec, between a lawyer or a notary and their client.

Appeal allowed, MCLACHLIN C.J. *and* CROMWELL J. *dissenting.*

Solicitors for the appellant: Stockwoods, Toronto.

Solicitor for the respondent: Public Prosecution Service of Canada, Toronto.

Solicitor for the intervener the Attorney General of Ontario: Attorney General of Ontario, Toronto.

Solicitors for the intervener the Canadian Civil Liberties Association: Torys, Toronto.

Solicitor for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: University of Ottawa, Ottawa.