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, s. 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

Société TELUS Communications *Appelante*

c.

Sa Majesté la Reine *Intimée*

et

Procureur général de l'Ontario, Association canadienne des libertés civiles et Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko *Intervenants*

Répertorié : R. *c.* Société TELUS Communications

2013 CSC 16

N° du greffe : 34252.

2012 : 15 octobre; 2013 : 27 mars.

Présents : La juge en chef McLachlin et les juges LeBel, Fish, Abella, Cromwell, Moldaver et Karakatsanis.

EN APPEL DE LA COUR SUPÉRIEURE DE JUSTICE DE L'ONTARIO

Droit criminel — Interception de communications — Mandat général — Messages textes stockés brièvement dans la base de données informatique d'une société de télécommunications par suite de la procédure particulière qu'elle applique pour les transmettre — Mandat général obligeant la société de télécommunications à communiquer prospectivement, sur une base quotidienne, tous les messages textes envoyés et reçus par deux abonnés — Le mandat général prévu à l'art. 487.01 du Code criminel peut-il autoriser la communication prospective de futurs messages textes se trouvant dans l'ordinateur d'un fournisseur de services? — La technique d'enquête autorisée par le mandat général délivré en l'espèce constitue-t-elle une interception qui doit être autorisée en vertu de la partie VI du Code criminel? — Un mandat général peut-il être délivré à bon droit lorsqu'une disposition législative en vigueur traite du contenu de la technique d'enquête, sinon de sa forme précise? — Code criminel, L.R.C. 1985, ch. C-46, art. 487.01.

Contrairement à la plupart des fournisseurs de services de télécommunications, la Société TELUS Communications a pour pratique de copier électroniquement tous les messages textes envoyés ou reçus par

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.

ses abonnés et de les conserver brièvement dans une base de données. En l'espèce, les policiers ont obtenu, en vertu des art. 487.01 et 487.02 respectivement du *Code criminel*, un mandat général et une ordonnance d'assistance connexe obligeant Telus à fournir aux policiers copie de tous les messages textes envoyés ou reçus par deux de ses abonnés et se trouvant dans sa base de données. L'extrait pertinent du mandat obligeait Telus à produire pendant deux semaines, sur une base quotidienne, tous les messages envoyés ou reçus. Telus a demandé l'annulation du mandat général, soutenant que la prise de connaissance prospective, sur une base quotidienne, de messages textes se trouvant dans sa base de données constitue une interception de communications privées et doit, en conséquence, être autorisée en vertu des dispositions de la partie VI du *Code* relatives à l'autorisation d'écoute électronique. La demande a été rejetée. Le pourvoi soulève la question de savoir si la communication prospective de futurs messages textes se trouvant dans l'ordinateur d'un fournisseur de services peut être autorisée en vertu du mandat général.

Arrêt (la juge en chef McLachlin et le juge Cromwell sont dissidents) : Le pourvoi est accueilli et le mandat général ainsi que l'ordonnance d'assistance connexe sont annulés.

Les juges LeBel, Fish et Abella : La partie VI du *Code criminel* instaure un régime complet d'« autorisation d'écoute électronique » en vue de l'interception de communications privées. La partie VI a pour objet de restreindre la capacité des policiers d'obtenir et de divulguer des communications privées.

Telus applique pour transmettre des messages textes une procédure particulière qui fait que ces messages sont stockés brièvement dans sa base de données informatique. Pour décider si la partie VI s'applique à la communication prospective, sur une base quotidienne, de futurs messages textes stockés dans l'ordinateur de Telus, il nous faut tenir compte de l'objectif général de cette partie VI.

La messagerie texte est, essentiellement, une conversation électronique. Les différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l'étendue de la protection accordée aux communications privées. La seule distinction entre la messagerie texte et les communications orales traditionnelles réside dans le processus de transmission. Cette distinction ne devrait pas avoir pour effet de priver les messages textes des mesures de protection des communications privées auxquelles ces messages ont droit sous le régime de la partie 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 any thing 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.

L'article 487.01 du *Code*, qui prévoit le mandat général, a été édicté en 1993 dans le cadre d'une série de modifications apportées au *Code* par le projet de loi C-109, L.C. 1993, ch. 40. Il habilite un juge à décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive ». L'alinéa 487.01(1)*c*) prévoit notamment que le pouvoir d'accorder un mandat général a un caractère résiduel et que son utilisation est interdite dans le cas où une autre disposition du *Code* ou d'une autre loi fédérale permet à un juge d'autoriser l'utilisation du dispositif, de la technique ou de la méthode proposé ou encore l'accomplissement de l'acte envisagé.

L'alinéa 487.01(1)*c*) doit être interprété largement de sorte que le mandat général ne soit pas utilisé comme mesure de premier recours, afin d'éviter que les autorités se soustraient aux exigences plus spécifiques ou rigoureuses en matière d'autorisation préalable, comme celles que l'on trouve à la partie VI. Il est nécessaire d'interpréter le terme « intercepter » à la partie VI afin de déterminer si l'al. 487.01(1)*c*) s'applique, c'est-à-dire si une autre disposition prévoit l'autorisation demandée. Le mot « intercepter » est utilisé dans toute la partie VI et se rapporte à l'interception de *communications privées*. Il faut par conséquent interpréter l'expression « intercepter une communication privée » en tenant compte de la vaste portée de la partie VI, du fait qu'elle s'applique à différentes plateformes technologiques, ainsi que de son objectif, à savoir la protection du droit individuel à la vie privée en matière de communication au moyen de garanties particulièrement strictes. Cette interprétation ne doit pas être dictée par le moyen technologique qui est employé pour transmettre de telles communications, par exemple l'ordinateur utilisé en l'espèce, mais plutôt par les aspects que le législateur a voulu protéger au moyen des dispositions de la partie VI. Cette interprétation doit se fonder aussi sur les droits garantis par l'art. 8 de la *Charte*, lesquels doivent progresser au rythme de la technologie.

Le fait d'interpréter de manière formaliste le mot « intercepter » aurait essentiellement pour effet de rendre la partie VI inutile en matière de protection du droit à la vie privée dans le cas des nouveaux moyens technologiques de communication textuelle électronique qui génèrent et sauvegardent des copies des communications privées dans le cadre du processus de transmission. Une interprétation étroite est en outre incompatible avec la formulation et l'objet de la partie VI qui accorde une protection étendue aux communications privées contre les ingérences non autorisées de l'État.

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

Il faut par conséquent interpréter les mots « intercepter une communication privée » en s'attachant à la prise de connaissance du contenu informationnel de la communication et aux attentes qu'avaient les interlocuteurs en matière de respect de la vie privée au moment de cette communication. Dans la mesure où le sens formaliste du mot « intercepter » pourrait comporter intrinsèquement un aspect temporel, cela ne devrait pas faire obstacle à l'intention du législateur de protéger, dans l'application de la partie VI, le droit des gens au respect de leur vie privée en matière de communications. L'emploi du mot « intercepter » implique que la prise de connaissance de la communication privée se fait au cours du processus de transmission. Ce processus englobe toutes les activités du fournisseur de services qui sont nécessaires ou accessoires à la fourniture du service de communication. La prise de connaissance de la substance d'une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications ferait, en conséquence, partie de ce processus.

Les messages textes constituent des communications privées et, même s'ils sont stockés dans l'ordinateur d'un fournisseur de services, la communication prospective de futurs messages de cette nature doit être autorisée en vertu de la partie VI du *Code*. Si Telus n'exploitait pas une base de données informatique, il ne fait aucun doute que les policiers seraient tenus d'obtenir une autorisation en vertu de la partie VI afin de recevoir prospectivement communication de messages textes, et ce, sur une base continue en l'espèce. La plupart des fournisseurs de services de transmission ne copient pas systématiquement les messages textes dans une base de données. Par conséquent, si la personne ciblée par les policiers était desservie par un fournisseur différent, ces derniers devraient nécessairement obtenir des autorisations d'écoute électronique sous le régime de la partie VI pour contraindre ce fournisseur à leur communiquer de façon prospective et continue les messages textes. Cette situation crée une injustice flagrante pour les personnes qui ne réalisent vraisemblablement pas que le choix de leur fournisseur de services de télécommunications peut avoir de sérieuses répercussions sur leur vie privée. Les différences techniques inhérentes à la procédure de transmission des messages textes propre à Telus ne devraient pas priver les abonnés de cette dernière des mesures de protection prévues par le *Code* et auxquelles ont droit tous les autres Canadiens.

Le mandat général en l'espèce était invalide parce que les policiers n'avaient pas respecté la condition prévue par l'al. 487.01(1)*c*) du *Code*, à savoir qu'un mandat général

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 preconditions. 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

ne peut être décerné si une autre disposition du *Code* permet d'autoriser la technique utilisée par les policiers. Comme le mandat entend autoriser l'interception de communications privées et que les interceptions de ce genre sont régies par le régime de la partie VI, un mandat général ne pouvait être délivré.

Les juges Moldaver et Karakatsanis : Il y a accord avec la juge Abella pour dire que la police n'a droit d'obtenir un mandat général que si elle est à même de démontrer qu'« aucune disposition » du *Code criminel* ou d'une autre loi fédérale n'autorise le recours à la technique, ou à un procédé équivalent en substance à la technique, pour laquelle l'autorisation est demandée. La technique d'enquête en l'espèce était équivalente sur le plan du fond à une interception. Par conséquent, le mandat général est invalide. Il n'est pas nécessaire de déterminer si ce qui s'est produit en l'espèce était ou non, à proprement parler, une « interception » au sens de l'art. 183 du *Code criminel*. Un motif de décision plus restreint nous met à l'abri des conséquences imprévues et incalculables dans ce domaine complexe du droit.

L'issue de l'espèce repose sur le défaut des autorités d'établir la condition prévue à l'al. 487.01(1)*c*) qu'il n'y ait « aucune disposition » permettant la fouille ou la perquisition. Cette disposition fait en sorte que le mandat général est utilisé avec modération et de façon limitée. En créant le mandat général, le législateur n'a pas supprimé les autres autorisations de fouille et de perquisition du *Code criminel* pour laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle comme ils l'entendent. Par conséquent, les tribunaux doivent veiller à combler le vide législatif uniquement lorsque le législateur n'a pas prévu une autorisation de fouille ou de perquisition en particulier. La condition qu'il n'y ait « aucune disposition » doit être interprétée de façon à accorder à la police la souplesse envisagée par le législateur lorsqu'il a créé le mandat général, tout en empêchant son utilisation abusive. Il est nécessaire de resserrer l'examen judiciaire lorsque le législateur a prévu une autorisation pour une technique d'enquête qui correspond, sur le plan du fond, à ce que la police cherche à obtenir, mais qui requiert des conditions préalables plus strictes. Par conséquent, le critère fondé sur l'al. 487.01(1)*c*) exige la prise en compte de la technique d'enquête que la police cherche à utiliser en fonction de son fond réel et non simplement de sa forme.

L'approche à l'égard de la condition qu'il n'y ait « aucune disposition » accepte un certain degré d'incertitude en chargeant les juges d'examiner au fond les techniques d'enquête censément « nouvelles ». En cas

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 preconditions. 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

d'incertitude, la police ferait bien de pécher par excès de prudence. Le mandat général ne peut être utilisé pour contourner d'autres dispositions applicables en matière d'autorisation, mais qui comportent des conditions préalables plus exigeantes. Les juges saisis d'une demande relative à une technique d'enquête qui, bien que non identique, s'apparente du point de vue du fond à une technique d'enquête prévue par une autre disposition pour laquelle des normes plus rigoureuses s'appliquent devraient redoubler de prudence. Si un examen minutieux établit qu'une technique d'enquête proposée, bien que similaire, est différente, sur le plan du fond, d'une technique existante, les juges peuvent accorder le mandat général en tenant compte de l'obligation que leur impose le par. 487.01(3) de fixer des modalités qui reflètent la nature du droit à la protection de la vie privée en jeu.

L'interprétation littérale de l'al. 487.01(1)*c*) doit être rejetée. Une telle interprétation vide la disposition de tout sens et lui fait perdre pratiquement toute valeur. L'historique législatif confirme que les mandats généraux devaient jouer un rôle modeste, en offrant à la police une voie constitutionnelle pour recourir à des techniques d'enquête que le législateur n'avait pas abordées. Veiller à ce que le recours aux mandats généraux soit limité constitue le véritable objet de l'al. 487.01(1)*c*). Bien que l'exigence que le mandat serve « au mieux » l'administration de la justice prévue à l'al. 487.01(1)*b*) vise à empêcher le recours abusif au mandat général, cette disposition ne devrait pas être interprétée comme englobant la question analytique distincte que pose le critère exigeant qu'il n'y ait « aucune disposition ». Une interprétation téléologique de l'al. 487.01(1)*c*) n'a rien à voir avec une nécessité pour l'enquête. Suivant la condition qu'il n'y ait « aucune disposition », la police n'est pas tenue de démontrer pourquoi une autre autorisation ne serait pas praticable au regard des faits d'une affaire en particulier, mais plutôt pourquoi elle est différente sur le plan du fond des autorisations déjà prévues par le législateur.

En l'espèce, le mandat général est invalide parce que la technique d'enquête qu'il autorisait était équivalente sur le fond à une interception. Ce que la police a fait — obtenir l'autorisation prospective de se faire transmettre des communications privées futures de façon continue, sinon constante, pendant une période prolongée — équivalait au fond à ce qu'elle aurait fait conformément à une autorisation visée à la partie VI. Cette transmission équivalait donc, à tout le moins, à une interception. Même si aucun élément de preuve ne laisse entendre que la police a agi autrement que de bonne foi, elle ne s'est pas acquittée de son fardeau de démontrer que la

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

technique contestée était différente sur le plan du fond d'une interception. D'après les faits de l'espèce, le mandat général n'a servi qu'à éviter la rigidité de la partie VI. La police aurait pu et aurait dû demander une autorisation sous le régime de la partie VI.

La juge en chef McLachlin et le juge Cromwell (dissidents) : La question de savoir si ce que la police a fait en vertu du mandat général constitue l'interception de communications privées relève de l'interprétation de la loi. À la lecture des dispositions législatives dans leur contexte intégral, il est clair que le mandat général ne permet pas une interception nécessitant une autorisation sous le régime de la partie VI. Si un message texte est incontestablement une communication privée et s'il est tout aussi incontestable que Telus a intercepté des messages textes au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, la police, en l'espèce, n'a pas intercepté ces messages lorsque Telus lui a remis copie des messages envoyés et reçus qu'elle avait préalablement interceptés et stockés dans ses bases de données. Par conséquent, la technique d'enquête autorisée en l'espèce par le mandat général n'est pas une interception de communications privées.

La distinction entre *l'interception* de communications privées et *la divulgation, l'utilisation ou la conservation* de communications privées qui ont été interceptées est fondamentale pour ce qui est de l'objet des dispositions relatives à l'écoute électronique et du régime qu'elles établissent. L'objet, le texte et le régime de la partie VI montrent que la divulgation, l'utilisation ou la conservation de communications privées interceptées sont distinctes de l'interception elle-même. En effet, si la divulgation ou l'utilisation d'une communication privée en constituait l'interception, il n'aurait pas été nécessaire de les ériger en infraction distincte. De la même façon, les exonérations de responsabilité criminelle prévues par le législateur indiquent qu'il a établi une distinction entre l'interception, d'une part, et la conservation, l'utilisation et la divulgation, d'autre part.

En l'espèce, nul ne conteste que Telus interceptait les messages textes lorsqu'elle les copiait pour les besoins de gestion de ses propres systèmes. Cela dit, il est pareillement reconnu que Telus a licitement intercepté des communications privées. En vertu du mandat général, la police a demandé à Telus la divulgation de renseignements que Telus avait déjà légalement interceptés. Le mandat général n'obligeait pas Telus à intercepter des communications, mais à fournir copie de communications qu'elle avait déjà interceptées à des fins licites qui lui étaient propres. Comme l'indique clairement

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

le régime législatif, la divulgation ou l'utilisation de communications interceptées légitimement ne constituent pas une interception. La conclusion que la police interceptait des communications privées en recevant de Telus des copies de messages textes déjà interceptés et stockés est incompatible avec la distinction fondamentale qu'établit le texte de loi. La distinction que fait la loi entre l'interception et la divulgation ne peut pas être qualifiée de simple « différence technique ». Elle constitue un élément fondamental du régime créé par les dispositions en cause. Lorsque Telus remet à la police les copies de communications déjà interceptées, elle les divulgue, elle ne les intercepte pas à nouveau. Cette divulgation par Telus de données stockées dans ses bases de données ne peut pas constituer une interception par la police.

On n'intercepte pas des communications déjà interceptées et stockées en en prenant connaissance, parce qu'une telle interprétation large est incompatible avec la nette distinction que font les dispositions législatives entre interception et divulgation. L'application générale de cette interprétation de « prendre volontairement connaissance » élargirait bien au-delà de tout ce qui a déjà pu être envisagé le champ des techniques d'enquête nécessitant une autorisation d'écoute électronique. En outre, introduire un aspect temporel à la notion d'interception confond l'acte d'intercepter et la nature de son autorisation. L'interception est une technique, une façon de prendre connaissance de la substance d'une communication privée. La même technique, donnant connaissance de l'information sous la même forme, ne peut pas constituer soit une saisie de renseignements stockés, soit une interception, selon le moment où elle est autorisée.

Le mandat général n'est pas une autorisation qu'il faut utiliser de façon limitée et avec modération. Au contraire, cette disposition est formulée en termes larges, ainsi que le signalent de nombreux auteurs. Par conséquent, la prémisse voulant que cet article doive être interprété de façon à en restreindre sévèrement l'utilisation est rejetée. L'examen porte sur deux points (outre, bien sûr, les motifs raisonnables de croire qu'une infraction a été commise et que l'autorisation demandée permettra d'obtenir des renseignements la concernant) : l'autorisation porte-t-elle sur l'utilisation d'« un dispositif ou une technique ou une méthode d'enquête » ou « l'accomplissement d'un acte » prévu par une autre disposition législative fédérale, et sert-elle au mieux l'administration de la justice? L'alinéa 487.01(1)*c*) prévoit qu'un mandat général peut être décerné « s'il n'y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou

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 by 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

une ordonnance permettant une telle utilisation [d'un dispositif, d'une technique ou d'une méthode d'enquête] ou l'accomplissement d'un tel acte ». Les mots « une telle utilisation [d'un dispositif, d'une technique ou d'une méthode d'enquête] » et « l'accomplissement d'un tel acte » renvoient tous à *ce que* la police veut faire, non aux *raisons* motivant ce choix. Cet alinéa n'exige pas que le juge saisi examine s'il existe des techniques analogues et si elles permettent d'obtenir les mêmes éléments de preuve, mais simplement si *une telle utilisation* peut être autorisée par une autre disposition. Il ne s'agit pas simplement d'une interprétation étroite et littérale de l'art. 487.01. Il s'agit plutôt d'une interprétation qui rend compte de son objet : l'octroi au juge du vaste pouvoir discrétionnaire d'autoriser la police « à utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte », pourvu, naturellement, que le juge soit convaincu que l'autorisation sert au mieux l'administration de la justice après avoir accordé l'importance voulue à la protection constitutionnelle contre les fouilles, perquisitions et saisies abusives. Un juge ne devrait toutefois pas autoriser tout ce que la police cherche à faire simplement parce que l'autorisation n'est pas prévue par un autre texte législatif. Son pouvoir discrétionnaire de décerner le mandat doit s'exercer en donnant pleinement effet à la protection des attentes raisonnables en matière de vie privée, comme l'établit l'art. 8 de la *Charte*.

L'inclusion à l'al. 487.01(1)*c*) d'un critère de « l'équivalent sur le plan du fond » n'est étayée ni par le texte de cette disposition, ni par son objet, ni par la jurisprudence. La question posée par cet alinéa est simple : Est-ce qu'une loi fédérale prévoit « un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte »? Lorsque cette condition préalable est respectée, le juge peut envisager d'accorder l'autorisation demandée. La question de savoir *s'il y a lieu* d'accorder l'autorisation demandée ne relève pas de cet alinéa. Pour déterminer s'il y a lieu de décerner un mandat général, il faut plutôt se tourner vers l'al. 487.01(1)*b*), lequel pose la question de savoir si la délivrance du mandat général servirait au mieux l'administration de la justice. Non seulement le texte et l'objet de la disposition de même que la jurisprudence étayent-ils une telle approche, mais l'application d'un critère de « l'équivalent sur le plan du fond » engendre une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d'autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives. La prévisibilité et la clarté du droit revêtent une importance

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 and Iannuzzi (No. 6)* (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

particulière en matière d'autorisation judiciaire préalable de fouilles et de perquisitions. L'autorisation préalable n'a pas pour but premier de détecter après le fait des fouilles ou perquisitions abusives, mais d'en prévenir l'existence. Les exigences en matière d'autorisation préalable doivent être aussi claires que possible pour assurer l'entière protection du droit garanti par la *Charte*.

La technique visée par la demande d'autorisation en l'espèce n'équivaut pas fondamentalement à l'autorisation de l'écoute électronique. Vu les faits de la présente espèce, l'autorisation d'écoute électronique seule ne permettrait pas à la police d'obtenir les renseignements que Telus devait fournir en exécution du mandat général. Il faudrait trois autorisations distinctes pour que la police ait accès à l'information qu'elle recevrait grâce au mandat général. Ainsi, même si l'on acceptait l'ajout par interprétation, à l'al. 487.01(1)*c*), d'un critère de « l'équivalent sur le plan du fond », ni les faits ni le droit n'étayent son application en l'espèce.

La demande de la police visant à obtenir un mandat général en l'espèce n'était pas une façon de contourner les exigences de la partie VI. Le mandat général permettait l'atteinte des objectifs légitimes de l'enquête policière de façon beaucoup plus pratique et économique que ce qui aurait pu être autorisé en vertu de toute autre disposition. Il n'y a aucune preuve de « recours abusif » à l'art. 487.01. Un service de police municipal de taille plutôt réduite a mené une enquête de façon efficace et pratique, en respectant pleinement le droit à la vie privée des personnes visées par l'enquête ainsi que des autres abonnés de Telus.

Jurisprudence

Citée par la juge Abella

Arrêts mentionnés : *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *R. c. Welsh and Iannuzzi (No. 6)* (1977), 32 C.C.C. (2d) 363; *Lyons c. La Reine*, [1984] 2 R.C.S. 633; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992; *R. c. Tse*, 2012 CSC 16, [2012] 1 R.C.S. 531; *R. c. Wong*, [1990] 3 R.C.S. 36; *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 R.C.S. 427.

Citée par le juge Moldaver

Arrêts mentionnés : *R. c. Wong*, [1990] 3 R.C.S. 36; *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751; *Lyons c. La Reine*, [1984] 2 R.C.S. 633; *R. c. Brand*, 2008

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, [2012] 3 S.C.R. 34; *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 (CanLII); *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

Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act, S.C. 1993, c. 40 (Bill C-109).

Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess., 41st Parl., 2011-12 (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., 2011-12-13 (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 [ad. 1993, c. 40, s. 15], 487.012, 487.02, 492.2(1), (2).

Interpretation Act, R.S.C. 1985, c. I-21, s. 35 "telecommunications" [am. 1993, c. 38, s. 87].

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.

BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *Schreiber c. Canada (Procureur général)*, [1997] 2 C.F. 176, inf. par [1998] 1 R.C.S. 841; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992.

Citée par le juge Cromwell (dissident)

Société Télé-Mobile c. Ontario, 2008 CSC 12, [2008] 1 R.C.S. 305; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241; *R. c. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. c. Cross*, 2007 CanLII 64141; *R. c. Little*, 2009 CanLII 41212; *R. c. Tse*, 2008 BCSC 906 (CanLII); *R. c. Weir*, 2001 ABCA 181, 281 A.R. 333; *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, autorisation d'appel refusée, [2009] 3 R.C.S. vii; *R. c. Lauda* (1998), 37 O.R. (3d) 513, conf. par [1998] 2 R.C.S. 683; *R. c. Noseworthy* (1997), 33 O.R. (3d) 641; *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*); *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 8, 24(2).

Code criminel, L.R.C. 1985, ch. C-46, partie VI, art. 183 « communication privée », « intercepter », 184, 184.4, 185, 186, 189, 193, 195, 196, 487, 487.01 [aj. 1993, ch. 40, art. 15], 487.012, 487.02, 492.2(1), (2).

Loi d'interprétation, L.R.C. 1985, ch. I-21, art. 35 « télécommunication » [mod. 1993, ch. 38, art. 87].

Loi modifiant le Code criminel, la Loi sur la responsabilité civile de l'État et le contentieux administratif et la Loi sur la radiocommunication, L.C. 1993, ch. 40 (projet de loi C-109).

Loi sur la protection de la vie privée, S.C. 1973-74, ch. 50.

Projet de loi C-30, *Loi sur la protection des enfants contre les cyberprédateurs*, 1re sess., 41e lég., 2011-2012 (Première lecture le 14 février 2012).

Projet de loi C-55, *Loi donnant suite à la décision de la Cour suprême du Canada dans l'affaire R. c. Tse*, 1re sess., 41e lég., 2011-2012-2013 (Première lecture le 11 février 2013).

Projet de loi C-176, *Loi sur la protection de la vie privée*, 1re sess., 29e lég., 1973, Notes explicatives.

Doctrine et autres documents cités

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*, 2nd ed. Toronto: Thomson Carswell, 2004.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, vol. 1. Toronto: Carswell, 2005 (loose-leaf updated 2012, release 7).

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

[1] Abella J. — 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

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*, 2nd ed. Toronto : Thomson Carswell, 2004.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, vol. 1. Toronto : Carswell, 2005 (loose-leaf updated 2012, release 7).

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.

POURVOI contre une décision de la Cour supérieure de justice de l'Ontario (le juge Sproat), 2011 ONSC 1143, 105 O.R. (3d) 411, [2011] O.J. No. 974 (QL), 2011 CarswellOnt 1331, qui a confirmé la validité d'un mandat général et d'une ordonnance d'assistance connexe. Pourvoi accueilli, la juge en chef McLachlin et le juge Cromwell sont dissidents.

Scott C. Hutchison, *Michael Sobkin* et *Fredrick Schumann*, pour l'appelante.

Croft Michaelson et *Lisa Matthews*, pour l'intimée.

Michal Fairburn, pour l'intervenant le procureur général de l'Ontario.

Wendy Matheson et *Rebecca Wise*, pour l'intervenante l'Association canadienne des libertés civiles.

Argumentation écrite seulement par *Tamir Israel*, pour l'intervenante la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko.

Version française du jugement des juges LeBel, Fish et Abella rendu par

[1] La juge Abella — Pour bon nombre de Canadiennes et de Canadiens, la messagerie texte est devenue une forme de communication de plus en plus populaire. Malgré certaines différences technologiques, elle présente plusieurs caractéristiques de la communication orale traditionnelle : elle se veut un moyen de conversation, la

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

transmission du message est généralement instantanée et l'on s'attend à ce que la communication demeure privée. La question en litige dans le présent pourvoi consiste à déterminer la procédure qui doit être appliquée par les tribunaux, en vertu du *Code criminel*, L.R.C. 1985, ch. C-46, pour autoriser la communication prospective, sur une base quotidienne, de tels messages se trouvant dans une base de données informatique exploitée par un fournisseur de services de télécommunications.

[2] En l'espèce, le fournisseur de services concerné est la Société TELUS Communications. Cette dernière invite la Cour à conclure que la prise de connaissance volontaire prospective, sur une base quotidienne, de messages textes se trouvant dans sa base de données constitue une interception de communications privées et doit, en conséquence, être autorisée en vertu de la partie VI du *Code*, laquelle instaure un régime complet d'« autorisation d'écoute électronique » en vue de l'interception de communications privées. Le ministère public soutient pour sa part que l'extraction de messages d'un ordinateur exploité par un fournisseur de services ne relève pas de la partie VI, parce que la production de messages stockés sur ordinateur ne constitue pas une « interception », et que les policiers peuvent par conséquent invoquer le mandat général prévu à l'art. 487.01 du *Code* pour être autorisés à obtenir copie de messages textes.

[3] La partie VI du *Code* établit un régime de protection des communications privées. Par suite de la procédure particulière que Telus applique pour transmettre des messages textes, ces messages sont stockés brièvement dans sa base de données informatique. La question qui se pose en l'espèce consiste à décider si, en raison des différences techniques inhérentes à la procédure de transmission des messages textes propre à Telus, les abonnés de cette dernière devraient être privés des mesures de protection prévues par le *Code* et auxquelles ont droit tous les autres Canadiens.

[4] Le nœud du présent pourvoi réside donc dans l'interprétation du mot « intercepter » utilisé à la partie VI. Dans toute cette partie, ce mot se rapporte à l'interception de *communications privées*.

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

Il faut par conséquent interpréter l'expression « intercepter une communication privée » en tenant compte de la vaste portée de la partie VI, du fait qu'elle s'applique à différentes plateformes technologiques ainsi que de son objectif, à savoir la protection du droit individuel à la vie privée en matière de communication au moyen de garanties particulièrement strictes. Cette interprétation ne doit pas être dictée par le moyen technologique qui est employé pour transmettre de telles communications, par exemple l'ordinateur utilisé en l'espèce, mais plutôt par les aspects que le législateur a voulu protéger au moyen des dispositions de la partie VI.

[5] La messagerie texte est, essentiellement, une conversation électronique. La seule distinction entre la messagerie texte et les communications orales traditionnelles réside dans le processus de transmission. Cette distinction ne devrait pas avoir pour effet de priver les messages textes des mesures de protection des communications privées auxquelles ces messages ont droit sous le régime de la partie VI. Les différences techniques intrinsèques des nouvelles technologies ne devraient pas déterminer l'étendue de la protection accordée aux communications privées.

Contexte

[6] Lorsqu'un abonné de Telus envoie un message texte, la transmission de ce message se déroule suivant la séquence d'opérations suivante : le message est d'abord transmis à la tour de transmission la plus proche, qui le relaie à l'infrastructure de transmission de Telus, d'où il est ensuite acheminé à la tour de transmission la plus proche du destinataire puis, enfin, au téléphone de ce dernier. Si l'appareil du destinataire est éteint ou hors de portée d'une tour de transmission, le message demeure temporairement dans l'infrastructure de transmission de Telus pendant une période maximale de cinq jours, après quoi Telus met fin aux tentatives de transmission et supprime le message sans en informer l'expéditeur.

[7] Contrairement à la plupart des fournisseurs de services de télécommunications, Telus a pour

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

pratique de copier électroniquement les messages textes envoyés ou reçus par ses abonnés et de les conserver dans une base de données pendant une période de 30 jours. Les messages textes envoyés par un abonné sont copiés dans la base de données à l'étape du processus de transmission où ils entrent dans l'infrastructure de transmission de Telus. Les messages textes que reçoit un abonné sont copiés lorsqu'ils parviennent à l'appareil de ce dernier. En raison de ce système, il arrive dans bien des cas que le message texte soit copié dans la base de données avant de parvenir à l'appareil du destinataire ou avant que ce dernier ne l'ait lu, ou les deux.

[8] Le 27 mars 2010, le service de police d'Owen Sound a obtenu un mandat général en vertu de l'art. 487.01, ainsi qu'une ordonnance d'assistance connexe en vertu de l'art. 487.02 du *Code*. Le mandat désignait deux abonnés des services mobiles de Telus et obligeait cette entreprise à fournir aux policiers copie de tous les messages textes envoyés ou reçus par ces abonnés qui étaient conservés dans la base de données de Telus. Le mandat exigeait en outre la production de renseignements relatifs aux abonnés permettant d'identifier toute personne ayant envoyé des messages textes aux deux personnes visées par le mandat ou ayant reçu de tels messages de ces personnes.

[9] Le mandat visait une période subséquente de deux semaines allant du 30 mars au 16 avril 2010, période pendant laquelle Telus devait observer un calendrier de communication précis. Le 30 mars 2010, Telus devait produire les renseignements se rapportant à la période du 18 au 30 mars 2010. Au cours de chacun des 13 jours suivants, elle devait produire, sur une base quotidienne, les messages textes envoyés ou reçus pendant les 24 heures précédentes, ainsi que tout renseignement connexe relatif aux abonnés.

[10] Telus a soutenu que le mandat était invalide parce que les policiers n'avaient pas respecté la condition prévue par l'al. 487.01(1)*c*) du *Code*, à savoir qu'un mandat général ne peut être décerné

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

si une autre disposition du *Code* permet d'autoriser la technique utilisée par les policiers. Comme le mandat entendait autoriser l'interception de communications privées et que les interceptions de ce genre sont régies par le régime de la partie VI, un mandat général ne pouvait être délivré. Pour sa part, le ministère public a plaidé que l'extraction de messages de cette base de données de Telus ne relevait pas de la partie VI, puisque les copies emmagasinées dans la base de données n'étaient pas des communications en temps réel et que, de ce fait, les policiers pouvaient demander un mandat général autorisant la production de futurs messages textes stockés dans la base de données d'un fournisseur.

[11] Le juge saisi de la demande a débouté Telus (2011 ONSC 1143, 105 O.R. (3d) 411). La partie du mandat visant la communication d'anciens messages antérieurs à la délivrance du mandat a été annulée, étant donné que tant le ministère public que Telus ont reconnu qu'il était possible de demander une ordonnance de communication afin d'obtenir ces messages.

[12] À mon avis, les messages textes constituent des communications privées et, même s'ils sont stockés dans l'ordinateur d'un fournisseur de services, la communication prospective de futurs messages de cette nature doit être autorisée en vertu de la partie VI du *Code*.

[13] Si Telus n'exploitait pas une base de données informatique, il ne fait aucun doute que les policiers seraient tenus d'obtenir une autorisation en vertu de la partie VI afin de recevoir prospectivement communication de messages textes, et ce, sur une base continue en l'espèce. En fait, la plupart des fournisseurs de services de transmission ne copient pas systématiquement les messages textes dans une base de données. Par conséquent, si la personne ciblée par les policiers était desservie par un fournisseur différent, ces derniers devraient nécessairement obtenir des autorisations d'écoute électronique sous le régime de la partie VI pour contraindre ce fournisseur à leur communiquer

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 any thing 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

de façon prospective et continue de futurs messages textes. Cette situation crée une injustice flagrante pour les personnes qui ne réalisent vraisemblablement pas que le choix de leur fournisseur de services de télécommunications peut avoir de sérieuses répercussions sur leur vie privée.

[14] Je suis donc d'avis d'accueillir le pourvoi et d'annuler le mandat général et l'ordonnance d'assistance connexe.

Analyse

[15] Il ne nous a pas été demandé de décider si un mandat général peut autoriser la communication de messages textes existants ou encore d'examiner l'application et la validité de la disposition régissant les ordonnances de communication en ce qui concerne les communications privées. Le présent pourvoi soulève plutôt la question de savoir si la communication *prospective* de futurs messages textes se trouvant dans l'ordinateur d'un fournisseur de services peut être autorisée en vertu du mandat général prévu à l'art. 487.01 du *Code*. Cela signifie que nous n'avons pas besoin de décider si la saisie de ces messages textes constituerait une interception si elle était autorisée après leur stockage.

[16] Édicté en 1993, l'art. 487.01 faisait partie d'une série de modifications apportées au *Code* par le projet de loi C-109, L.C. 1993, ch. 40. Ce projet de loi a instauré plusieurs nouvelles dispositions en matière d'autorisation judiciaire. L'article 487.01 a pour objectif de permettre l'obtention de mandats de perquisition à l'égard de techniques ou méthodes non précisées dans le *Code*. Il habilite un juge à décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive » :

487.01 (1) Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l'article 552 peut décerner un mandat par écrit autorisant un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une

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 (*sub nom. R. v. Ford*), at para. 50).

[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

méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l'égard d'une personne ou d'un bien :

> *a*) si le juge est convaincu, à la suite d'une dénonciation par écrit faite sous serment, qu'il existe des motifs raisonnables de croire qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l'infraction seront obtenus grâce à une telle utilisation ou à l'accomplissement d'un tel acte;
>
> *b*) s'il est convaincu que la délivrance du mandat servirait au mieux l'administration de la justice;
>
> *c*) *s'il n'y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte.*

[17] La solution du présent pourvoi dépend de la question de savoir si l'al. 487.01(1)*c*) s'applique à la présente situation, en d'autres mots s'il existe une autre disposition permettant d'obtenir l'autorisation qui est sollicitée en l'espèce. Dans *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, le juge MacPherson a fait remarquer que l'analyse fondée sur l'al. 487.01(1)*c*) s'attache à [TRADUCTION] « la technique ou méthode d'enquête particulière que la police veut utiliser et à la question de savoir si cette technique ou méthode peut être autorisée par une autre disposition du Code ou d'une autre loi fédérale » (par. 43; voir aussi *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*), par. 50).

[18] Par conséquent, il ressort d'un examen contextuel de l'al. 487.01(1)*c*) que le pouvoir d'accorder un mandat général a un caractère résiduel et que son utilisation est *interdite* dans le cas où une autre disposition du *Code* ou d'une autre loi fédérale permet à un juge d'autoriser l'utilisation du dispositif, de la technique ou de la méthode proposé ou encore l'accomplissement de l'acte envisagé.

[19] Autrement dit, l'al. 487.01(1)*c*) doit être interprété largement de sorte que le mandat général ne soit pas utilisé comme mesure de premier

the circumvention of more specific or rigorous pre-authorization requirements for warrants (S. C. Hutchison et al., *Search and Seizure Law in Canada* (loose-leaf), 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

recours. Il a pour but d'éviter que les autorités se soustraient aux exigences plus spécifiques ou rigoureuses en matière d'autorisation préalable (S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), p. 16-40.3).

[20] Cela signifie que le ministère public a droit à un mandat général uniquement lorsqu'il est en mesure de prouver qu'aucune autre disposition ne prévoit un mandat, une autorisation ou une ordonnance permettant le recours à la technique en question, y compris, comme le souligne le juge Moldaver, quelque disposition autorisant des techniques équivalentes, sur le plan du fond, à celle proposée par les policiers dans une affaire donnée. La technique d'enquête autorisée par le mandat général délivré en l'espèce a permis à la police d'obtenir directement d'un fournisseur de services, et ce, chaque jour pendant une période de deux semaines, la communication prospective de futurs messages textes. L'argument du ministère public consiste essentiellement à dire qu'il était impossible de recourir à une autre disposition, étant donné que l'extraction de messages stockés ne constituait pas une interception. Si le ministère public a raison, il a droit à la délivrance d'un mandat général. S'il a tort, le mandat général qui a été délivré doit être annulé. D'une manière ou d'une autre, il est essentiel de déterminer si la technique que la police voulait employer devait être autorisée sous le régime de la partie VI.

[21] Le ministère public n'a à aucun moment concédé que les circonstances de la présente espèce donnaient ouverture soit à un mandat général soit à une autorisation fondée sur la partie VI. Il a plutôt affirmé que la condition prévue à l'al. 487.01(1)*c*) était respectée, vu l'absence d'autre disposition permettant d'obtenir la communication prospective de futurs messages textes stockés dans l'ordinateur d'un fournisseur de services, la partie VI n'étant pas selon lui applicable du fait que l'extraction de messages stockés dans un ordinateur ne constitue pas une « interception ». Il s'agit là de la question centrale à trancher en l'espèce.

[22] La Cour doit donc décider si la partie VI s'applique à la communication prospective — et, en

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 and Iannuzzi (No. 6)* (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

l'espèce, continue — des messages textes demandés par la police ou si, du fait que ces messages sont stockés dans l'ordinateur de Telus, leur extraction ne constitue pas une « interception ». Si la partie VI s'applique, un mandat général ne peut alors être décerné, conformément à l'al. 487.01(1)*c*).

[23] Aux termes du par. 184(1), constitue un acte criminel le fait d'« intercept[er] volontairement une communication privée » au moyen d'un dispositif. La partie VI établit un régime exhaustif pourvoyant à l'autorisation de telles interceptions. Ces dispositions ont été édictées en 1974 par la *Loi sur la protection de la vie privée*, S.C. 1973-74, ch. 50, qui a modifié le *Code* en y ajoutant la partie IV.1 (aujourd'hui la partie VI) intitulée « Atteintes à la vie privée ». Le juge Zuber a expliqué ainsi l'objet de ces dispositions dans *R. c. Welsh and Iannuzzi (No. 6)* (1977), 32 C.C.C. (2d) 363 (C.A. Ont.) :

> [TRADUCTION] Il est évident qu'en édictant la *Loi sur la protection de la vie privée*, 1973-74 (Can.), ch. 50, [. . .] le Parlement visait deux objectifs. Le premier était de protéger les communications privées en interdisant leur interception et en rendant inadmissible la preuve obtenue en violation de cette loi. Le second objectif, qui fait contrepoids au premier, était de reconnaître la nécessité de permettre aux autorités compétentes, sous réserve de certaines restrictions précises, d'intercepter des communications privées dans le cadre d'une enquête sur un crime grave et de produire la preuve ainsi obtenue. [p. 369]

[24] Parce qu'elle a pour objet de restreindre la capacité des policiers d'obtenir et de divulguer des communications privées, la partie VI est rédigée en termes généraux afin d'assurer la protection nécessaire. Dans l'arrêt *Lyons c. La Reine*, [1984] 2 R.C.S. 633, la Cour a expliqué ainsi la portée de ces dispositions :

> Il s'agit d'un texte législatif général qui vise, par ces dispositions étendues, l'utilisation de toute une gamme de dispositifs radioélectriques, téléphoniques, optiques et acoustiques pour écouter et enregistrer les communications privées dont une définition générale est donnée. Il ne s'agit ni d'un texte législatif portant sur le branchement clandestin de lignes téléphoniques ou sur l'écoute clandestine, ni d'un règlement sur la radio.

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

Il s'agit d'une réglementation de toutes ces choses et de « tout autre dispositif » qui peut servir à intercepter des renseignements dont l'auteur peut raisonnablement s'attendre à ce qu'ils ne soient pas interceptés par une personne autre que celle à laquelle il les destine. [p. 664]

[25] Suivant la définition qui en est donnée à l'art. 183, le mot « intercepter » s'entend notamment « du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ». Il s'agit là d'une définition non exhaustive, qui cadre avec la portée large de la partie VI et met l'accent sur la prise de connaissance par l'État du contenu informationnel — substance, sens ou objet — de la communication privée. Ce n'est pas seulement la communication elle-même qui est protégée, mais aussi toute information connexe à cette communication qui permet d'en dégager la substance ou le sens. L'expression « communication privée » est définie ainsi à l'art. 183 :

Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

[26] Cette définition souligne les attentes raisonnables de l'auteur de la communication en matière de respect de sa vie privée à cet égard. Le mot « télécommunication » figurant dans la définition est lui-même défini en ces termes dans la *Loi d'interprétation*, L.R.C. 1985, ch. I-21, art. 35, modifié en 1993 (L.C. 1993, ch. 38, art. 87) : « La transmission, l'émission ou la réception de signes, signaux, écrits, images, sons ou renseignements de toute nature soit par système électromagnétique, notamment par fil, câble ou système radio ou optique, soit par tout procédé technique semblable ».

[27] Les articles 185 et 186 du *Code* énoncent les exigences générales applicables aux demandes

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

d'autorisation présentées en vertu de la partie VI. En comparaison des conditions prévues par d'autres dispositions du *Code* se rapportant aux fouilles, saisies, perquisitions et mandats, ces articles comportent des exigences plus strictes au titre de la protection de la vie privée. Avant d'accorder une autorisation fondée sur la partie VI, le juge doit être convaincu que cette mesure sert au mieux l'administration de la justice.

[28] Le juge doit également être convaincu, conformément à l'al. 186(1)*b*), que « d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête ». Dans *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992, la Cour a précisé que cette exigence obligeait la police à démontrer qu'il n'existait « aucune autre méthode d'enquête raisonnable dans les circonstances de l'enquête criminelle considérée » (par. 29).

[29] Les autorisations décernées en vertu de la partie VI doivent aussi indiquer l'identité des personnes dont les communications privées seront interceptées, le lieu où les communications seront interceptées et la façon dont elles le seront. Les autorisations doivent également préciser les modalités que le juge estime opportunes, et elles ne sont valides que pour une période maximale de 60 jours. Enfin, la demande doit être présentée par écrit par le procureur général, le ministre de la Sécurité publique ou un mandataire spécialement désigné.

[30] Outre ces conditions préalables d'autorisation, la partie VI énonce un certain nombre d'exigences en matière d'avis. L'article 196 requiert que soient « avisées », dans un certain délai, les personnes ayant fait l'objet d'interceptions autorisées en vertu de l'art. 186. Suivant l'art. 189, l'accusé doit être avisé de toute interception dont on entend présenter les fruits en preuve. De plus, l'art. 195 oblige le ministre de la Sécurité publique et de la Protection civile ou le procureur général de chaque province à établir chaque année un rapport sur l'utilisation des autorisations visées à la

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

partie VI. Dans *R. c. Tse*, 2012 CSC 16, [2012] 1 R.C.S. 531, la Cour a jugé que l'obligation de notification assure la transparence du processus et constitue une mesure de contrôle supplémentaire à l'égard du pouvoir de la police d'exécuter des interceptions très attentatoires en matière de communications privées. Elle a en conséquence conclu qu'une disposition de notification était nécessaire au respect des normes constitutionnelles minimales établies par l'art. 8 de la *Charte canadienne des droits et libertés*.

[31] Ces garanties font bien ressortir l'intention du législateur d'accorder une protection plus grande aux communications privées. La partie VI s'applique largement à divers moyens technologiques et prévoit des garanties plus strictes que d'autres dispositions du *Code* en matière de mandat. Il nous faut donc tenir compte de cet objectif général pour décider si la partie VI s'applique à la communication prospective, sur une base quotidienne, de futurs messages textes stockés dans l'ordinateur de Telus.

[32] Comme l'ont reconnu les parties, les messages textes sont clairement visés par la définition de « télécommunication » figurant dans la *Loi d'interprétation*. Les parties ont également reconnu que, tout comme les communications orales, ces messages surviennent dans des circonstances faisant naître une attente raisonnable en matière de respect de la vie privée et constituent, de ce fait, des « communication[s] privée[s] » au sens de l'art. 183. En outre, il ne fait pas de doute que l'ordinateur utilisé par Telus est visé par les mots « [t]out dispositif » à l'art. 183.

[33] La question consiste donc à interpréter le mot « intercepter » à la partie VI. L'interprétation de ce mot doit se fonder non seulement sur les objectifs de la partie VI, mais aussi sur les droits garantis par l'art. 8 de la *Charte*, lesquels doivent progresser au rythme de la technologie. Dans *R. c. Wong*, [1990] 3 R.C.S. 36, la Cour a conclu que « le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 [de la *Charte*] doit évoluer au rythme du progrès technologique et, par conséquent, nous

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

assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés » (p. 44). Le fait d'interpréter de manière formaliste le mot « intercepter » aurait essentiellement pour effet de rendre la partie VI inutile en matière de protection du droit à la vie privée dans le cas des nouveaux moyens technologiques de communication textuelle électronique qui génèrent et sauvegardent des copies des communications privées dans le cadre du processus de transmission.

[34] Il est vrai que, contrairement aux communications orales traditionnelles, un message texte n'est pas toujours communiqué à son destinataire au moment où il est créé. La réception d'un tel message texte suppose que le téléphone soit ouvert et se trouve à la portée d'une tour de transmission, et que le destinataire consulte le message. Si Telus ne parvient pas à transmettre un message, celui-ci demeure dans son infrastructure de transmission pendant cinq jours, après quoi Telus met fin à ses tentatives de transmission. En outre, contrairement aux communications orales, les communications textuelles — qui sont, de par leur nature, des écrits — génèrent un document qui peut facilement être copié et conservé. Une interprétation étroite ou formaliste du mot « intercepter », qui exigerait que l'interception ait lieu en même temps que la communication elle-même, est donc dépourvue d'utilité pour étudier les nouvelles communications textuelles électroniques.

[35] Une interprétation étroite est en outre incompatible avec l'objet de la partie VI et les termes généraux qui y sont utilisés. La définition française d'« intercepter » à l'art. 183 comporte trois aspects distincts : « écouter », « enregistrer » et « prendre [. . .] connaissance ». La définition législative élargit la notion d'« intercepter » au lieu de la limiter à son sens étroit et technique. La définition de ce mot dans le *Code* n'exige aucunement que l'interception d'une communication privée s'effectue simultanément à la communication elle-même ou sensiblement au même moment. Si le législateur avait voulu établir une telle exigence, il l'aurait fait dans la définition d'« intercepter ». Il a plutôt choisi d'adopter une définition plus générale, conforme à

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

l'objet de la partie VI, qui consiste à accorder une protection étendue aux communications privées contre les ingérences non autorisées de l'État.

[36] Il faut par conséquent interpréter les mots « intercepter une communication privée » en s'attachant à la prise de connaissance du contenu informationnel de la communication et aux attentes qu'avaient les interlocuteurs en matière de respect de la vie privée au moment de cette communication. À mon avis, dans la mesure où le sens formaliste du mot « intercepter » pourrait comporter intrinsèquement un aspect temporel, cela ne devrait pas faire obstacle à l'intention du législateur de protéger, dans l'application de la partie VI, le droit des gens au respect de leur vie privée en matière de communications.

[37] L'emploi du mot « intercepter » implique que la prise de connaissance de la communication privée se fait au cours du processus de transmission. À mon avis, ce processus englobe toutes les activités du fournisseur de services qui sont nécessaires ou accessoires à la fourniture du service de communication. La prise de connaissance de la substance d'une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications ferait, en conséquence, partie de ce processus.

[38] Mettre l'accent sur le fait que le *Code* établit une distinction entre l'interception de communications privées et leur divulgation ne permet pas d'offrir la protection qu'est censée accorder la partie VI. Au contraire, cela fait en sorte que les différences d'ordre technologique du processus de transmission employé par Telus font échec à la protection qu'entendait accorder le législateur aux communications privées contre les atteintes étatiques.

[39] La réalité des technologies modernes de communication fait en sorte que des communications privées électroniques, par exemple des messages textes, sont souvent à la fois en cours de transmission *et* simultanément stockées sur ordinateur, sous une certaine forme, par le fournisseur de services. Par conséquent, la même communication

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).

privée se trouve à plus d'un endroit, ce qui permet à l'État d'en prendre connaissance à partir du canal de transmission et de l'ordinateur où elle est stockée. Autrement dit, la même communication privée peut être « interceptée » par la police plus d'une fois à partir de sources différentes.

[40] Quand Telus copie des messages dans sa base de données informatique, plusieurs étapes du processus de transmission n'ont pas encore été réalisées. Il découle du calendrier de communication fixé par le mandat général en l'espèce que les policiers ont vraisemblablement obtenu des copies stockées de certains messages textes avant même leur réception par la personne à laquelle ils étaient destinés. Le ministère public concède que, si les policiers avaient pris connaissance de ces mêmes communications privées directement à partir du canal de transmission plutôt que des copies stockées, l'autorisation prévue à la partie VI aurait été nécessaire. Le degré de protection accordé ne devrait pas dépendre du fait que l'État prend connaissance soit d'une copie de la communication privée en cours de transmission soit d'une copie stockée par un fournisseur de services dans le cadre du processus de communication. Le législateur a rédigé la partie VI en termes larges, de façon à ce que les communications privées soient protégées sur plusieurs plateformes technologiques (voir *Lyons*).

[41] Le processus de communication qu'emploie un tiers fournisseur de services ne devrait pas faire échec à la protection que le législateur entend accorder aux communications privées. Comme l'ont souligné dans leur mémoire les intervenantes l'Association canadienne des libertés civiles et la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, la Cour a reconnu dans d'autres contextes que les fournisseurs de services de télécommunications ne sont que des tiers qui transmettent des communications privées à titre d'« agents » et qu'ils devraient pouvoir fournir leurs services sans que cela n'entraîne d'effets juridiques sur la nature (ou, en l'espèce, sur la protection) de ces communications (*Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, 2004 CSC 45, [2004] 2 R.C.S. 427, par. 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

[42] La partie VI reconnaît les dangers inhérents au fait de permettre l'accès aux futures communications privées d'un nombre potentiellement illimité de personnes pendant une longue période. Il s'agit là exactement des risques que soulève intrinsèquement la technique d'enquête utilisée en l'espèce. Une autorisation permettant à la police d'obtenir la communication *prospective* de *futurs* messages textes pendant une période de deux semaines, directement à partir du processus de communication employé par le fournisseur de services, constitue précisément le genre de situations auxquelles la protection de la partie VI est censée s'appliquer. À mon avis, la technique d'enquête en cause est une « interception de communications privées » visée à la partie VI.

[43] La définition d'« intercepter » à l'art. 183 appuie une interprétation des mots « intercepter une communication privée » qui englobe la technique d'enquête utilisée par la police en l'espèce. Cette définition inclut la simple prise de connaissance d'une communication. Elle n'exige pas qu'il soit pris connaissance de la communication elle-même; la prise de connaissance « de sa substance, son sens ou son objet » suffit. En outre, cette interprétation s'harmonise avec l'esprit et l'objet de la partie VI, laquelle est rédigée en termes larges de manière à régir et à encadrer une grande variété d'atteintes technologiques à la vie privée. Enfin, elle établit l'équilibre voulu entre l'atteinte grave à la vie privée qui résulte de la prise de connaissance clandestine de communications privées, et l'évolution des besoins en matière d'application efficace de la loi.

[44] Les policiers ont joui d'un avantage considérable en recourant au mandat général. Ils n'avaient pas besoin d'une demande d'autorisation présentée par le procureur général; ils n'étaient pas tenus de démontrer que d'autres méthodes d'enquête avaient été utilisées sans succès; ils n'avaient pas l'obligation d'aviser les personnes ciblées; ils n'avaient pas à préciser l'identité des autres personnes dont les communications privées risquaient d'être regardées au cours de l'enquête.

[45] Le mandat général décerné en l'espèce visait à permettre une technique d'enquête déjà

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 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

envisagée par la procédure d'autorisation d'écoute électronique prévue à la partie VI, c'est-à-dire permettre à la police d'obtenir la production *prospective* de *futures* communications privées à partir d'un ordinateur exploité par un fournisseur de services dans le cadre de son processus de transmission. Comme la partie VI s'appliquait, le mandat général prévu à l'art. 487.01 ne pouvait être décerné.

[46] En conséquence, je suis d'avis d'accueillir le pourvoi et d'annuler le mandat général et l'ordonnance d'assistance connexe.

Version française des motifs des juges Moldaver et Karakatsanis rendus par

LE JUGE MOLDAVER —

I. Introduction

[47] Lorsqu'une technique d'enquête policière va à l'encontre de l'attente raisonnable d'une personne en matière de vie privée, il revient au législateur d'autoriser spécifiquement la technique. Il s'agit là de la règle générale. La disposition du *Code criminel*, L.R.C. 1985, ch. C-46, portant sur ce qu'on a appelé le « mandat général » fait exception à la règle et permet à la police de s'adresser au tribunal pour qu'il autorise une technique d'enquête proposée qui n'est pas expressément autorisée par la loi. Parmi les questions soulevées en l'espèce, à mon avis, la question décisive consiste à savoir si un mandat général peut être dûment décerné lorsque le fond d'une technique d'enquête, sinon sa forme précise, est déjà visé par une autre disposition législative en vigueur.

[48] J'ai eu l'occasion de lire les motifs de ma collègue la juge Abella et, bien que nous abordons la question différemment, je suis d'accord avec elle pour conclure que le mandat général en l'espèce est invalide. Les motifs de ma collègue s'attachent principalement à la définition d'« intercepter » qui figure à l'art. 183 du *Code* et à la question de savoir si la fouille en l'espèce était visée par cette définition pour l'application de la partie VI. Je ne crois pas qu'il soit nécessaire de répondre à ces

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

questions parce que, à mon sens, l'issue de l'espèce repose sur le défaut des autorités d'établir l'une des conditions d'autorisation nécessaires à l'obtention d'un mandat général.

[49] Au vu des faits de l'espèce, si l'on se détache de la forme et qu'on examine sur le fond la fouille que la police désirait effectuer, on se retrouve avec ce qui équivaut à une interception au sens de la partie VI. À ce titre, la police aurait pu — et aurait dû, comme je vais l'expliquer — demander une autorisation sous le régime de la partie VI, ce qui empêche la délivrance d'un mandat général. Par conséquent, je suis d'avis, comme ma collègue la juge Abella, d'accueillir le pourvoi et d'annuler le mandat général ainsi que l'ordonnance d'assistance connexe.

II. Aperçu des questions soulevées dans le présent pourvoi

[50] Les arguments principaux des parties au pourvoi ont trait à la question de savoir si la technique d'enquête autorisée par le mandat général entre dans la définition d'« intercepter » à l'art. 183 du *Code*. Les parties conviennent que s'il y a eu interception en l'espèce, le mandat général ne pouvait être décerné, faute de respecter la condition, prévue à l'al. 487.01(1)*c*) du *Code*, qu'il n'y ait « aucune disposition » qui prévoie le mandat. Bien entendu, elles divergent d'opinion sur la question de savoir si cette technique constitue une interception.

[51] Ma collègue la juge Abella et moi sommes d'avis que le ministère public n'a droit d'obtenir un mandat général que s'il est à même de démontrer qu'« aucune disposition » n'autorise le recours à la technique, ou à un procédé équivalent en substance à la technique, proposée par la police dans une affaire donnée. Nous partageons également le même avis sur l'issue de l'espèce, mais nous divergeons d'opinion sur la manière d'y parvenir.

[52] Ma collègue estime que la technique d'enquête en l'espèce *constituait* une interception au sens de l'art. 183; elle est donc d'avis de déclarer invalide le mandat général. Je préfère plutôt trancher la présente affaire en partant du principe

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

que la technique d'enquête qui nous occupe *était équivalente, sur le plan du fond*, à une interception et, à la lumière de cette conclusion, je suis également d'avis de déclarer invalide le mandat général.

[53] J'emprunte une voie différente parce que j'hésite à me servir de la présente affaire pour analyser ce qui constitue une interception pour l'application de la partie VI. En envisageant la question comme je le fais, je suis conscient de la nécessité d'écarter les menaces que présente l'ère numérique pour la vie privée. Adapter des lois édictées dans les années 1970 à un univers de téléphones intelligents et de réseaux sociaux est une tâche difficile et profondément importante. Mais il ne m'apparaît pas nécessaire de déterminer si ce qui s'est produit en l'espèce était ou non une interception à proprement parler parce qu'il existe un motif de décision plus restreint qui nous met à l'abri des conséquences imprévues et incalculables dans ce domaine complexe du droit.

III. Analyse

A. *La disposition relative au mandat général*

[54] En 1993, le législateur a édicté la disposition relative au mandat général ainsi que plusieurs nouveaux pouvoirs en matière de fouille et de perquisition en réponse à une série de décisions de notre Cour concernant la surveillance électronique. L'article 487.01 a été adopté précisément pour répondre à l'arrêt *R. c. Wong*, [1990] 3 R.C.S. 36. Dans cet arrêt, la Cour a conclu que la surveillance vidéo par la police d'activités qui se déroulent dans une chambre d'hôtel va à l'encontre de l'attente raisonnable d'une personne en matière de vie privée et nécessite ainsi une autorisation judiciaire préalable conformément à une disposition législative valide. La réponse du législateur, qui a pris la forme de l'art. 487.01, allait au-delà de l'autorisation de la surveillance vidéo. La disposition prévoit en partie ce qui suit :

487.01 (1) [Dénonciation pour mandat général] Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l'article 552 peut décerner un mandat par écrit autorisant

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

un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l'égard d'une personne ou d'un bien :

a) si le juge est convaincu, à la suite d'une dénonciation par écrit faite sous serment, qu'il existe des motifs raisonnables de croire qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l'infraction seront obtenus grâce à une telle utilisation ou à l'accomplissement d'un tel acte;

b) s'il est convaincu que la délivrance du mandat servirait au mieux l'administration de la justice;

c) s'il n'y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte.

(2) [Limite] Le paragraphe (1) n'a pas pour effet de permettre de porter atteinte à l'intégrité physique d'une personne.

(3) [Fouilles, perquisitions ou saisies raisonnables] Le mandat doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances.

[55] La portée du mandat général — soit l'autorisation judiciaire d'« utiliser un dispositif ou une technique ou une méthode d'enquête » ou d'« accomplir tout acte » qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive — est restreinte par de nombreuses conditions préalables à sa délivrance et par des modalités d'exécution. La principale de ces conditions, et celle qui, à mon sens, est au cœur du présent pourvoi, est celle, prévue à l'al. 487.01(1)*c*), qu'il n'y ait « aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte ».

[56] La condition qu'il n'y ait « aucune disposition » autorisant la fouille ou la perquisition

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

fait en sorte que le mandat général est utilisé avec modération et de façon limitée. Cette condition permet d'éviter que le mandat général ne devienne [TRADUCTION] « un moyen détourné de recourir facilement à d'autres techniques dont les conditions préalables à l'autorisation sont plus exigeantes » : S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), p. 16-40.3. Sans vouloir prêter à la police des intentions malveillantes, j'estime que c'est ce qui s'est produit en l'espèce.

B. *Le mandat général en l'espèce*

[57] Dans un cas typique où la Société TELUS Communications (« Telus »), le fournisseur de services de télécommunications en l'espèce, reçoit signification d'une autorisation visée par la partie VI, elle installe un appareil qui copie automatiquement toutes les activités qui concernent le numéro de téléphone indiqué, y compris tous les messages textes, et transmet automatiquement ces données au service des télécommunications de la police. Le ministère public ne conteste pas que l'acquisition de cette façon de messages textes d'une personne constitue une interception au sens de la partie VI; il est admis également qu'un message texte peut constituer une « communication privée » au sens de la partie VI.

[58] Comme pratique d'entreprise, toutefois, Telus conserve systématiquement pendant au moins 30 jours dans ses bases de données une copie des messages textes envoyés et reçus par ses abonnés. Bien que Telus soit la seule, parmi les principaux fournisseurs de services de télécommunications, à faire de telles copies, elle a légalement le droit de le faire conformément à l'exception prévue au par. 184(2) du *Code*. La société affirme qu'elle intercepte les messages de ses abonnés de cette façon pour aider à résoudre les problèmes techniques de ses clients.

[59] Le fait que Telus conserve les messages textes de ses abonnés de cette façon est important — il constitue en fait le fondement du présent pourvoi — parce qu'il crée une ressource d'enquête pour les autorités. Comme l'a affirmé le sergent-détective

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 (for historic messages) or wiretap authorizations (for future messages)" (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

Prosser de la Police provinciale de l'Ontario dans son affidavit déposé à la Cour, la pratique de Telus [TRADUCTION] « permet aux enquêteurs d'accéder au contenu de ces messages par un autre moyen » (d.a., p. 115). Au moyen de mandats de perquisition ordinaires (art. 487) ou d'ordonnances de communication (art. 487.012), la police a déjà obtenu copie de messages conservés dans la base de données de Telus.

[60] En somme, avant la présente affaire, toutes les fouilles policières qui exigeaient les copies de messages textes d'abonnés de Telus étaient autorisées, à quelques exceptions près, soit sous le régime de la partie VI, soit par un mandat de perquisition ou une ordonnance de communication. Dans son mémoire, le ministère public résume la question : à l'égard des abonnés de Telus, la police demande généralement [TRADUCTION] « des mandats de perquisition ou des ordonnances de communication (relativement aux messages existants) ou des autorisations d'écoute électronique (relativement aux messages futurs) » (m.i., par. 10 (je souligne)).

[61] Le mandat général en l'espèce représente donc une troisième possibilité. Sur le plan de la forme, il ressemble à une ordonnance de communication, car il permet à la police d'avoir accès aux messages textes *déjà conservés dans la base de données de Telus*. Sur le plan du fond, il ressemble plutôt à l'autorisation visée par la partie VI, car il permet *prospectivement* à la police d'accéder à des communications privées *futures* de façon *continue* pendant une période prolongée.

[62] Le caractère hybride inhérent au mandat général en l'espèce fait ressortir la nécessité, pour le juge, de déterminer si la condition qu'il n'y ait « aucune disposition » est respectée pour examiner au fond la technique d'enquête policière, et non simplement ses formalités. Mais ce n'est pas ce qui s'est produit en l'espèce.

C. *Le mandat général a-t-il été valablement décerné?*

[63] Le juge siégeant en révision a examiné la jurisprudence de la Cour d'appel de l'Ontario. Dans

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

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.

R. c. Ha, 2009 ONCA 340, 96 O.R. (3d) 751, le juge MacPherson a indiqué ce qui suit :

> [TRADUCTION] L'analyse relative à l'al. 487.01(1)*c*) ne porte pas sur l'existence d'autres techniques d'enquête qui pourraient répondre aux besoins ou aux objectifs d'enquête de la police; elle porte plutôt sur la technique ou méthode d'enquête particulière que la police cherche à utiliser et sur la possibilité que cette utilisation puisse être autorisée par une autre disposition du Code ou d'une autre loi fédérale. [Je souligne; par. 43.]

[64] S'appuyant sur l'arrêt *Ha*, le juge siégeant en révision a conclu qu'aucune disposition, dans le *Code* ou dans une autre loi, n'autoriserait la technique d'enquête utilisée en l'espèce — à savoir la [TRADUCTION] « communication quotidienne de messages textes futurs » (2011 ONSC 1143, 105 O.R. (3d) 411, par. 75). Bien que la police « aurait pu s'adresser à un juge de paix tous les jours durant les 14 jours couverts par le mandat général et obtenir les mêmes enregistrements au moyen d'un mandat ordinaire », le mandat général pouvait être décerné précisément parce qu'il autorisait entièrement, à lui seul, la fouille que le législateur n'avait pas par ailleurs prévue (par. 70)[1].

[65] À mon humble avis, l'analyse est incomplète. Il va de soi que la police *aurait pu* demander une autorisation visée à la partie VI et atteindre ainsi l'objectif de son enquête. L'avocat du ministère public l'a d'ailleurs admis à l'audition du présent pourvoi :

> [TRADUCTION] Je ne suis pas certain s'ils ont bien réfléchi en fin de compte à la question parce que si ce que la police fait constitue une interception au sens de la partie VI, elle pourrait probablement s'adresser de nouveau au juge qui a décerné le mandat, soit un juge de la Cour supérieure, et lui demander une autorisation visée à la partie VI. [Je souligne; transcription, p. 81.]

Au vu du dossier dont dispose la Cour, la police n'a pas expliqué pourquoi elle n'aurait pas pu

1 La validité d'une série d'ordonnances de communication quotidiennes (ou plus fréquentes) n'a pas été contestée par les parties. Il n'est pas non plus nécessaire d'examiner cette question pour trancher le présent pourvoi. Par conséquent, je ne déterminerai pas si la Constitution ou une loi empêche la police de solliciter des ordonnances de cette nature.

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 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:

> . . . as 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. . . . [I]t 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

demander une autorisation visée par la partie VI. Nous savons que, n'eût été la pratique de Telus de conserver systématiquement les messages de ses abonnés, la police n'aurait pas eu d'autres choix que d'obtenir une telle autorisation puisqu'elle demandait l'autorisation prospective d'obtenir la communication quotidienne de messages textes futurs. En effet, c'est ce qu'elle fait — apparemment sans problème — avec les autres principaux fournisseurs de services de télécommunications, comme Rogers et Bell, qui ne conservent pas les messages textes comme le fait Telus.

[66] Quoi qu'il en soit, il reste à déterminer si, selon la loi, la police *aurait dû* demander une telle autorisation. À l'audience du présent pourvoi, l'avocat du ministère public a affirmé que l'arrêt *Ha* répond irréfutablement à la question par la négative :

> [TRADUCTION] . . . comme l'a indiqué la Cour d'appel de l'Ontario dans l'arrêt *Ha*, le critère à appliquer pour déterminer si un mandat général peut être décerné porte principalement sur la nature de la technique d'enquête en question, et non sur la nature de l'objectif de l'enquête.
>
> La fouille de la base de données de Telus visant à obtenir des enregistrements futurs est une technique qui est complètement distincte de la saisie d'une télécommunication. C'est-à-dire que du point de vue de la mécanique [. . .] les policiers ne faisaient pas la même chose. [. . .] [I]l s'agissait d'un processus complètement différent. [Je souligne; transcription, p. 94-95.]

[67] En toute déférence, je ne saurais être d'accord. Interpréter l'arrêt *Ha* de cette façon reviendrait à fermer les yeux sur le fond de la fouille — et sur le bon sens. Ce que la police a fait en l'espèce — obtenir l'autorisation *prospective* de se faire transmettre des communications privées *futures* de façon *continue*, sinon constante, pendant une période prolongée — équivalait au fond à ce qu'elle aurait fait conformément à une autorisation visée à la partie VI. Cette transmission équivalait donc, à tout le moins, à une interception.

[68] J'accepte la prétention du ministère public selon laquelle, sur le plan de la forme, les événements survenus en l'espèce diffèrent de ce qui se produirait conformément à une autorisation visée à

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

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.

la partie VI. Toutefois, je n'accepte pas que ce fait soit déterminant eu égard aux intérêts identiques en matière de vie privée. Abstraction faite du délai de 24 heures, les techniques d'enquête étaient les mêmes. Si l'on accepte la logique du ministère public, un mandat général aurait été décerné si le délai avait été de 24 minutes ou, d'ailleurs, de 24 secondes[2]. Établir une distinction entre ce qui a été autorisé en l'espèce et une interception au sens de la partie VI sur le fondement d'une telle théorie revient à établir « une distinction artificielle et irréaliste » : *Lyons c. La Reine*, [1984] 2 R.C.S. 633, p. 643.

[69] Par conséquent, il convient d'établir une distinction entre les faits de l'espèce et ceux de l'arrêt *Ha.* Tant l'arrêt *Ha* que l'arrêt *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*), l'autre arrêt d'une cour d'appel qui interprète l'art. 487.01, concernent des tentatives infructueuses par la personne visée par la fouille d'invalider un mandat général au motif que la police aurait pu demander plusieurs mandats ordinaires. Dans l'arrêt *Ha*, la police enquêtait sur un présumé laboratoire de fabrication de drogues. Elle a demandé l'autorisation de pénétrer clandestinement dans la propriété en tout temps dans une période de deux mois et d'y mener une vaste gamme d'activités de collecte d'éléments de preuve, notamment de prendre des photos, des échantillons de produits chimiques et de prélever des empreintes digitales sur des objets. De même, dans l'arrêt *Brand*, la police enquêtait sur d'importantes activités liées à la culture de marijuana et avait besoin de pénétrer secrètement dans diverses propriétés

2 Il n'est ni prudent ni nécessaire d'établir précisément en l'espèce à quel moment le délai modifierait la technique de la fouille sur le fond de façon à ce qu'un mandat général soit acceptable. Quel que soit le délai, l'intervalle de 24 heures en l'espèce était insuffisant. Dans la mesure où une affaire ultérieure présente une incertitude, elle doit être dissipée conformément à l'interprétation de l'al. 487.01(1)*c*) formulée en l'espèce. Je relève en outre que mon collègue le juge Cromwell insiste beaucoup sur le fait que « la réception de certains messages qui devaient être remis à la police pouvait être décalée de 72 heures, non de 24 heures » (par. 183). Avec égards, je ne comprends pas pourquoi il insiste sur ce fait. Même à supposer qu'un délai de 72 heures diffère d'une interception sur le plan du fond, il ne s'ensuit pas pour autant que l'autorisation intégrale doive être maintenue en vigueur parce qu'un élément d'une autorisation par ailleurs illégale est valide.

techniques for 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 that 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.

pour vérifier la présence de drogues sans compromettre d'autres aspects de son enquête. Fondamentalement, dans chaque cas, la demande d'accès en secret et la souplesse des délais démontraient clairement que le *fond* des techniques d'enquête pour lesquelles une autorisation était demandée différait de ce qui pouvait être autorisé dans le cadre d'un mandat ordinaire.

[70] Pour expliquer en quoi la fouille autorisée par le mandat général dans l'arrêt *Ha* était différente, sur le plan du fond, d'une fouille nécessitant plusieurs mandats ordinaires, le juge MacPherson a affirmé ce qui suit :

> [TRADUCTION] En l'espèce, la police a demandé l'autorisation d'effectuer un nombre illimité d'entrées et de fouilles clandestines dans une propriété privée sur une période de deux mois. À part l'art. 487.01 du Code, il n'y a « aucune disposition dans [. . .] toute autre loi fédérale » qui pourrait potentiellement permettre à la police d'accomplir ces actes. [par. 43]

Les faits dont nous sommes saisis sont tout autres. Dans le cas qui nous occupe, la police cherchait à obtenir, comme l'a dit le juge siégeant en révision, l'autorisation pour [TRADUCTION] « la technique ou la procédure d'enquête visant la communication prospective et quotidienne de messages textes » (par. 75). Mais en réalité, il *existe* une disposition qui prévoit au fond cette technique. Il s'agit de la partie VI.

[71] Pour souligner l'importance de regarder au-delà de la forme d'une technique d'enquête pour découvrir son fond véritable, il convient d'observer un autre point. Dans les arrêts *Ha* et *Brand*, si la police voulait obtenir des éléments de preuve, elle pouvait choisir entre une série de mandats ordinaires ou un mandat général. Si la police demandait un mandat général, il aurait fallu qu'elle respecte les conditions de l'art. 487.01, lesquelles sont délibérément plus strictes que celles relatives au mandat ordinaire. Par exemple, les conditions prévoyant qu'un mandat général ne peut être décerné que par un juge, et non par un juge de paix, et que sa délivrance doit servir au mieux l'administration de la justice visent à faire en sorte que le mandat général demeure un mandat d'arrière-garde auquel il faut limiter le recours.

[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).

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) and 186(6)).

3. A Part VI authorization is available only where "other investigative procedures have been tried and have failed, other investigative procedures

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.

[72] Autrement dit, les exigences plus strictes du mandat général dissuadent les autorités d'y recourir quotidiennement. Dans les arrêts *Ha* et *Brand*, où la seule autre solution consistait en une série de mandats ordinaires, le fait que la police a eu recours à un mandat général ne lui a pas permis de se soustraire facilement aux exigences d'une autorisation législative plus stricte — le mandat général *constituait* l'autorisation législative plus stricte. Dans ces deux arrêts, il est donc plus difficile de voir comment les dispositions portant sur le mandat général auraient pu être utilisées abusivement.

[73] En l'espèce, par contre, la police pouvait réellement choisir entre une autorisation visée à la partie VI et un mandat général[3]. Pour la police, les avantages étaient donc nettement différents de ceux dans l'arrêt *Ha*. Bien que le mandat général et les dispositions de la partie VI exigent que le juge soit convaincu que l'ordonnance sert au mieux l'administration de la justice, la partie VI à elle seule impose plusieurs autres exigences afin de protéger le droit au respect de la vie privée :

1. l'autorisation visée à la partie VI ne peut être obtenue que relativement à certaines infractions (art. 183);

2. seules les personnes désignées par le ministre de la Sécurité publique et de la Protection civile ou par le procureur général peuvent demander une autorisation visée à la partie VI (par. 185(1) et 186(6));

3. l'autorisation visée à la partie VI peut être obtenue uniquement lorsque « d'autres méthodes d'enquête ont été essayées et ont échoué, ou

3 Le dossier en l'espèce porte à croire que tous les renseignements sollicités par la police auraient pu être obtenus conformément à une autorisation visée par la partie VI, à l'autorisation d'utiliser un enregistreur de numéro sur le fondement du par. 492.2(1) et à une ordonnance en vue d'obtenir un registre de téléphone fondée sur le par. 492.2(2). Devant notre Cour, aucune des parties ne s'est penchée sur ces deux dernières autorisations; les parties se sont plutôt attardées sur la question de savoir si l'essence du mandat — la communication de messages textes — constituait une interception.

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

ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête » (al. 186(1)*b*));

4. l'autorisation visée à la partie VI doit indiquer l'identité des personnes dont les communications privées seront interceptées, le lieu où l'interception se fera et la façon dont on y procédera (al. 186(4)*c*));

5. le procureur général ou le ministre est tenu, dans un certain délai, d'aviser de l'autorisation la personne en cause (art. 196);

6. le ministre est tenu de présenter au Parlement un rapport annuel indiquant le nombre de demandes d'autorisation présentées sous le régime de la partie VI et les détails de ces demandes (art. 195).

[74] Par conséquent, en l'espèce, le fait de s'en tenir uniquement au mécanisme de la fouille nous fait perdre de vue l'essentiel. Le mandat général doit être comparé à l'autorisation visée à la partie VI lorsque l'on analyse les avantages qu'il offre à la police. L'interprétation mécanique de la condition qu'il n'y ait « aucune disposition » ne saurait être retenue parce que, pour dire les choses sans détour, un mandat général peut s'avérer plus facile à obtenir qu'une autorisation visée à la partie VI. Pour cette raison, on peut difficilement reprocher à la police de demander un mandat général au lieu d'une autorisation visée à la partie VI. Elle avait peu à perdre (un retard dans la réception des données sollicitées, qui aurait probablement eu peu de conséquences) et beaucoup à gagner (aucune obligation de s'acquitter du lourd fardeau que le législateur a choisi d'imposer sous le régime de la partie VI).

[75] Les faits portent à croire que c'est précisément ce qui s'est produit par suite du rejet de la contestation du mandat soulevée par Telus en l'espèce. Dans son affidavit, le sergent-détective Prosser affirme que la police demande des mandats généraux uniquement dans ces [TRADUCTION] « rares

"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. *The 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 preconditions.

circonstances » qui nécessitent l'accès aux messages textes « dans un délai plus court » (d.a., p. 116). Et pourtant, bien que Telus ait obtenu seulement six mandats généraux avant 2010, l'avocat de la société a informé la Cour à l'audience que le nombre a depuis augmenté à [TRADUCTION] « plusieurs centaines » depuis la décision de première instance (transcription, p. 42).

[76] La logique qui a mené à ce résultat prévisible annule en fait la mesure de protection exigeant qu'il n'y ait « aucune disposition » en invitant la police à différencier une technique d'enquête d'une certaine façon — de quelque façon que ce soit, même si la distinction est sans importance du point de vue du fond — afin d'éviter la rigidité d'une autorisation législative plus exigeante comme celle visée à la partie VI. Si la police doit choisir entre demander une autorisation sous le régime de la partie VI et procéder par un moyen moins exigeant, elle choisira sans doute la dernière option — ce qui est compréhensible. Par conséquent, je suis d'avis qu'il faut renforcer le critère exigeant qu'il n'y ait « aucune disposition » afin qu'il puisse répondre à son objectif de veiller à ce que le mandat général ne devienne pas une façon d'éviter le recours aux autorisations de fouille qui comportent des conditions plus exigeantes.

D. *Résumé de la façon d'aborder la condition qu'il n'y ait « aucune disposition »*

[77] Le critère fondé sur l'al. 487.01(1)*c*) exige la prise en compte de la technique d'enquête que la police cherche à utiliser en fonction de son fond réel et non simplement de sa forme. La disposition doit être interprétée de façon à accorder à la police la souplesse envisagée par le législateur lorsqu'il a créé le mandat général, tout en empêchant son utilisation abusive. Comme le démontrent les faits de l'espèce, il est nécessaire de resserrer l'examen judiciaire lorsque le législateur a prévu une autorisation pour une technique d'enquête qui correspond, sur le plan du fond, à ce que la police cherche à obtenir, mais qui requiert des conditions préalables plus strictes.

[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 preconditions.

[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

[78] En concluant ainsi, je souligne qu'en créant le mandat général, le législateur n'a pas supprimé les autres autorisations de fouille du *Code* pour laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle comme ils l'entendent. Par conséquent, les tribunaux doivent veiller à combler le vide législatif uniquement lorsque le législateur n'a pas prévu une autorisation de fouille en particulier. Agir autrement éroderait le fondement qui encadre les rôles respectifs des tribunaux et du législateur dans notre système de justice criminelle lorsque les droits et libertés d'une personne sont en jeu.

[79] Cela dit, je reconnais, comme je me dois de le faire, que cette approche accepte un certain degré d'incertitude en chargeant les juges d'examiner au fond les techniques d'enquête censément « nouvelles ». À mon avis, une interprétation qui demeure fidèle à l'objectif de la condition qu'il n'y ait « aucune disposition », prévue à l'al. 487.01(1)*c*), n'exige forcément pas moins. Toutefois, deux directives pratiques devraient servir à répondre aux questions qui peuvent être soulevées.

[80] Premièrement, il importe pour la police de comprendre que le mandat général n'est pas un mandat d'application générale. Au contraire, il doit être utilisé avec modération, lorsque la technique d'enquête que la police désire utiliser est réellement différente, sur le plan du fond, d'une technique d'enquête prévue par une disposition législative. En cas d'incertitude, la police ferait bien de pécher par excès de prudence. Elle doit savoir — avec certitude — que le mandat général ne peut être utilisé pour contourner d'autres dispositions applicables en matière d'autorisation, mais qui comportent des conditions préalables plus exigeantes.

[81] Deuxièmement, lorsque les juges sont saisis d'une demande en vue d'obtenir un mandat général et que la technique d'enquête, bien que non identique, s'apparente du point de vue du fond à une technique d'enquête prévue par une autre disposition pour laquelle des normes plus rigoureuses s'appliquent, ils devraient redoubler de prudence. À tout le moins, les juges devraient examiner attentivement les documents présentés et s'assurer

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.

que la demande en vue d'obtenir un mandat général est authentique et ne constitue pas seulement un moyen de contourner les exigences d'une autre disposition en matière d'autorisation. Si un examen minutieux établit qu'une technique d'enquête proposée, bien que similaire, est différente sur le plan du *fond* d'une technique existante — qui n'est pas simplement similaire du point de vue du fond, mais différente sur le plan de la forme — les juges peuvent accorder le mandat général, mais ils devraient tenir compte de l'obligation que leur impose le par. 487.01(3), c'est-à-dire qu'ils devraient fixer des modalités et conditions qui reflètent la nature du droit à la protection de la vie privée en jeu. Pour ce faire, ils peuvent s'inspirer des conditions que le législateur a choisi d'imposer à l'autorisation existante similaire sur le plan du fond.

[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*.

[82] À la lumière de ces deux considérations, et malgré les préoccupations du juge Cromwell à propos de la certitude, sur lesquelles je reviendrai, si la police a procédé de bonne foi et le juge fait preuve de prudence, il est peu probable qu'un mandat général décerné dans de telles circonstances soit jugé entaché d'un vice au procès — et encore moins que la preuve obtenue conformément à ce mandat soit exclue sur le fondement du par. 24(2) de la *Charte canadienne des droits et libertés*.

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

E. *La façon opposée de voir l'exigence qu'il n'y ait « aucune disposition »*

[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.

[83] J'ai eu l'occasion de lire les motifs du juge Cromwell, qui est d'avis que la condition qu'il n'y ait « aucune disposition » a été respectée en l'espèce parce que la technique d'enquête ne cadre pas dans la définition d'une « interception » pour l'application de la partie VI. Par conséquent, il est d'avis de rejeter le pourvoi. En ce qui concerne la définition d'une interception, l'analyse de mon collègue repose sur la distinction entre l'interception d'une communication privée (art. 184) et la divulgation subséquente de la communication ainsi interceptée (art. 193). Comme je l'ai expliqué, je ne crois pas qu'il soit nécessaire de me pencher sur cette question dans le présent pourvoi et, pour cette raison, je ne ferai aucun commentaire sur cet aspect de ses motifs.

[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 of 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 precondition 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:

[84] Toutefois, mon collègue conteste mon interprétation de l'al. 487.01(1)*c*) et son application au cas qui nous occupe. Il ne fait aucun doute que mon collègue et moi avons une vision fondamentalement différente non seulement de la condition qu'il n'y ait « aucune disposition », mais aussi du rôle des mandats généraux de manière plus générale. Il a fait une analyse minutieuse qui mérite une réponse.

[85] Le juge Cromwell affirme que l'al. 487.01 (1)*c*) devrait être interprété littéralement et rejette l'approche téléologique que j'ai adoptée, affirmant qu'elle « engendre [. . .] une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d'autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives » (par. 171). Selon mon collègue, « la prévisibilité et la clarté du droit revêtent une importance particulière en matière d'autorisation judiciaire préalable de fouilles et de perquisitions » (par. 172).

[86] Le juge Cromwell conteste aussi mon interprétation de l'al. 487.01(1)*c*) au motif qu'elle ajoute d'une manière inacceptable une « nécessité pour l'enquête » comme condition préalable supplémentaire à la délivrance d'un mandat général — à savoir que, pour obtenir un mandat général, la police doit être en mesure de démontrer qu'elle ne peut atteindre son objectif d'enquête par aucun autre moyen. Mon collègue affirme que le législateur n'a pas jugé bon d'ajouter une telle exigence et qu'il est inadmissible pour la Cour de le faire.

[87] Je propose de répondre à chacune des préoccupations du juge Cromwell.

[88] Premièrement, pour des raisons qui devraient ressortir clairement de ce qui précède, je ne saurais accepter l'interprétation littérale que donne mon collègue à l'al. 487.01(1)*c*). À mon humble avis, une telle interprétation vide la disposition de tout sens et lui fait perdre pratiquement toute valeur. En 1996, peu après l'introduction du mandat général, l'auteur d'un traité faisant autorité sur ce sujet a prédit ce qui suit :

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.]

[TRADUCTION] Des quatre conditions préalables [au mandat général], la plus difficile pour les enquêteurs sera [la condition qu'il n'y ait « aucune disposition »], une nouvelle disposition visant à empêcher que ce pouvoir résiduel de décerner un mandat ne devienne un moyen détourné de recourir facilement à d'autres techniques dont les conditions préalables à l'autorisation sont plus strictes. [Je souligne; Hutchison et autres, p. 16-40.3.]

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

Toutefois, l'approche de mon collègue aurait pour effet de réduire cette disposition à un tigre de papier.

[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.

[89] Selon l'interprétation littérale que mon collègue donne à l'al. 487.01(1)*c*), pour respecter la condition qu'il n'y ait « aucune disposition », il suffit d'une déviation — si légère ou insignifiante soit-elle — faisant en sorte qu'une technique d'enquête excède le cadre d'application d'une autre disposition en matière d'autorisation du *Code* ou d'une loi fédérale. Par conséquent, en l'espèce, si la police avait sollicité un mandat général obligeant Telus à fournir des copies de tous les messages textes conservés dans un délai de 24 secondes (au lieu de 24 heures), j'ai l'impression que mon collègue aurait conclu que la condition qu'il n'y ait « aucune disposition » avait été respectée. De même, selon l'interprétation de mon collègue, si la police avait sollicité un mandat général nécessitant l'interception *simultanée* des messages textes *et* un mandat autorisant le placement sous enregistreur de numéro, il semblerait que cela aussi aurait suffi pour respecter la condition qu'il n'y ait « aucune disposition ».

[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.

[90] Si, selon le raisonnement de mon collègue, le législateur avait vraiment voulu que la police puisse satisfaire à la condition qu'il n'y ait « aucune disposition » en trouvant un moyen détourné — n'importe lequel — qui ferait en sorte que la technique d'enquête excéderait le cadre d'application d'une autorisation existante, il nous faut alors conclure que le législateur a choisi d'édicter une disposition absurde. Je ne saurais accepter une telle 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

[91] Qui plus est, l'importance que mon collègue accorde à la grande portée de la disposition prévoyant le mandat général — une portée que je reconnais d'emblée — confond les questions

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 (C.A.), 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]" (S. C. Hutchison, *Hutchison's Canadian Search Warrant Manual 2005* (2nd ed. 2004), 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

distinctes de *ce* que le pouvoir permet de faire, à supposer qu'on puisse l'exercer, et *les moments* auxquels il peut être exercé. Comme je l'ai déjà indiqué, la disposition prévoyant le mandat général ne visait pas à effacer toutes les autres dispositions du *Code* en matière d'autorisation et à laisser aux juges le soin de concevoir les mandats généraux de façon ponctuelle. Au contraire, les mandats généraux ont été créés « pour combler toute "lacune" potentielle » (*Schreiber c. Canada (Procureur général)*, [1997] 2 C.F. 176 (C.A.), par. 86 (je souligne), inf. pour d'autres motifs par [1998] 1 R.C.S. 841), pour fournir une [TRADUCTION] « sécurité législative » qui « complète plutôt que remplace » (S. C. Hutchison, *Hutchison's Canadian Search Warrant Manual 2005* (2e éd. 2004), p. 143 et 163 (je souligne)), pour [TRADUCTION] « combler une lacune de l'enquête » (J. A. Fontana et D. Keeshan, *The Law of Search and Seizure in Canada* (8e éd. 2010), p. 459 (je souligne)), et pour servir de [TRADUCTION] « pouvoir résiduel » (Hutchison et autres, p. 16-36 (je souligne)).

[92] Bien que peu de choses aient été dites sur les mandats généraux dans les débats ou les audiences du comité en 1993, nous savons que le législateur n'a pas mis un terme à son intervention dans le domaine des mandats après avoir édicté l'art. 487.01. De multiples autorisations ont été créées depuis lors, notamment des ordonnances de communication en 2004. Des autorisations existantes ont été modifiées, y compris les dispositions de la partie VI, pour répondre aux besoins d'enquête en constante évolution et aux préoccupations quant à la vie privée. Et même aujourd'hui, le législateur continue d'examiner des propositions en matière de mandat présentées — et parfois retirées — par le gouvernement. Voir, p. ex., le projet de loi C-30, *Loi sur la protection des enfants contre les cyberprédateurs*, 1re sess., 41e lég. (Première lecture le 14 février 2012); le projet de loi C-55, *Loi donnant suite à la décision de la Cour suprême du Canada dans l'affaire R. c. Tse*, 1re sess., 41e lég. (Première lecture le 11 février 2013).

[93] Cet historique confirme que les mandats généraux devaient jouer un rôle modeste, en offrant à la police une voie constitutionnelle pour recourir

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 para. (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

à des techniques d'enquête que le législateur n'avait pas abordées. Ils constituaient donc des mandats d'arrière-garde auxquels il faut limiter le recours, et non des mandats de première ligne d'application générale. Ils devaient permettre de combler des lacunes, non en créer.

[94] Bref, veiller à ce que le recours aux mandats généraux soit limité constitue, à mon avis, le véritable objet de l'al. 487.01(1)*c*). L'interprétation littérale que donne le juge Cromwell à la disposition dénature cet objectif en invitant la police à demander aux tribunaux d'autoriser des techniques d'enquête censément « nouvelles » sur le fondement de distinctions dénuées de sens sur le plan du fond. De toute évidence, cette interprétation fait primer la forme aux dépens du fond.

[95] Mon collègue invoque la condition de servir « au mieux » l'administration de la justice, dont fait état l'al. 487.01(1)*b*), qui serait une mesure de protection suffisante contre le recours abusif au mandat général. Il prétend que le législateur a édicté l'al. (1)*b*) pour remédier à lui seul aux « recours potentiellement abusifs au mandat général » (par. 190). Mais s'il en est ainsi, il faut se demander pourquoi alors le législateur a édicté l'al. 487.01(1)*c*).

[96] Certes, l'exigence que le mandat serve « au mieux » l'administration de la justice vise à empêcher le recours abusif au mandat général. Mais cette disposition ne devrait pas être interprétée comme englobant la question analytique distincte que pose le critère exigeant qu'il n'y ait « aucune disposition ». Le rôle de chaque disposition doit être respecté. D'abord, suivant l'al. 487.01(1)*c*), il faut se demander s'il y a, dans le *Code* ou toute autre loi fédérale, une disposition qui prévoit en fait ou sur le fond la technique d'enquête que la police demande l'autorisation d'utiliser. Ensuite, suivant l'al. 487.01(1)*b*), ce n'est que si l'on répond par la négative à la première question qu'il faut se demander si la délivrance du mandat servirait au mieux l'administration de la justice.

[97] Les deux exemples que j'ai évoqués plus tôt illustrent ce point. Je souhaiterais qu'un délai

delay and a dial number recorder warrant piggybacked 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 para. (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.

de 24 secondes et un mandat autorisant l'utilisation d'un enregistreur de numéro combiné à une autorisation pour l'interception simultanée de messages textes répondraient à la définition de recours abusif que propose mon collègue. Pourquoi? Parce que l'on constaterait probablement la vraie nature des deux techniques d'enquête — l'équivalent, sur le plan du fond, d'une autorisation visée à la partie VI. À la fin, tous les chemins mènent à Rome. Mais l'interprétation de l'al. 487.01(1)*c*) à laquelle je souscris donne un certain sens et une utilité à la disposition; l'interprétation de mon collègue la dépouille des deux.

[98] En ce qui concerne l'al. 487.01(1)*b*), prenons, à titre d'exemple seulement, le fait que le recours à l'autorisation visée par la partie VI est limité à certaines infractions visées par la définition du terme « infraction » à l'art. 183. Si la police demande l'autorisation pour une fouille ou une perquisition concernant une infraction qui n'est pas visée par cette définition, bien que la condition qu'il n'y ait « aucune disposition » serait respectée, l'autorisation ferait l'objet d'une analyse fondée sur l'al. (1)*b*) pour prévenir la délivrance d'un mandat que le législateur a manifestement anticipé et délibérément exclu : S. Coughlan, « *R. v. Ha* : Upholding General Warrants without Asking the Right Questions » (2009), 65 C.R. (6th) 41, p. 41-43.

[99] Cela dit, mon collègue ne fournit aucune indication quant au genre de conduite qu'il qualifierait d'abusive, même s'il souligne que « le juge saisi d'une demande de mandat général doit veiller à ce que toute technique d'enquête autorisée respecte entièrement le droit à la protection contre les fouilles, perquisitions et saisies abusives » (par. 189). Vraisemblablement, il laisserait aux juges le soin de trancher la question de façon ponctuelle suivant l'al. 487.01(1)*b*), acceptant ainsi sa propre forme d'incertitude dans le processus. Je reconnais que l'approche fondée sur le fond à laquelle je souscris n'est pas hermétique — mais elle n'est pas plus perméable que l'approche fondée uniquement sur le recours au critère exigeant que le mandat serve « au mieux » l'administration de la justice auquel souscrit mon collègue.

[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

[100] Je me penche maintenant sur la deuxième préoccupation de mon collègue — selon laquelle j'ai introduit d'une manière inacceptable dans l'art. 487.01 une nécessité pour l'enquête, un concept propre à la partie VI. À mon humble avis, ma façon d'interpréter l'al. 487.01(1)*c*) n'a rien à voir avec une nécessité pour l'enquête.

[101] L'exigence prévue à l'al. 186(1)*b*) selon laquelle l'autorisation visée à la partie VI est nécessaire porte sur une question *factuelle*. En exigeant que d'autres méthodes « ont été essayées et ont échoué », ou qu'elles ont « peu de chance de succès » ou que « l'urgence de l'affaire est telle qu'il ne serait pas pratique » de les utiliser, il appert que l'al. 186(1)*b*) porte sur la question de savoir si les circonstances factuelles d'une affaire en particulier nécessitent l'exercice des pouvoirs conférés par la partie VI. Le juge LeBel l'a expliqué au nom de la Cour dans *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992 :

> Le législateur et les tribunaux ont en effet reconnu que l'interception des communications privées est une mesure grave, qui ne doit être envisagée que pour des infractions graves, que s'il existe des motifs probables et que s'il est véritablement nécessaire de recourir à l'écoute électronique compte tenu de l'enquête en cause et de ses objectifs [. . .] Sur le plan pratique, il ne doit exister aucune autre méthode d'enquête raisonnable, dans les circonstances de l'enquête criminelle considérée. [Je souligne; soulignement dans l'original omis; par. 29.]

[102] Par contre, la condition qu'il n'y ait « aucune disposition » soulève une question *juridique*. Il ne s'agit pas de savoir si d'autres techniques de fouille ont été épuisées, ou si elles ont peu de chance de succès, ou s'il y a urgence dans les circonstances. La question est plutôt de savoir si la technique d'enquête censément « nouvelle » est équivalente, en fait ou sur le fond, à une technique qui est déjà autorisée par la loi. Autrement dit, suivant la condition qu'il n'y ait « aucune disposition », la police n'est pas tenue de démontrer pourquoi une autre autorisation *ne serait pas praticable* au regard des faits d'une affaire en particulier, mais plutôt pourquoi elle est *différente sur le plan du fond* des autorisations déjà prévues par le législateur. Bien que le fait qu'une autre

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.

autorisation qui répondra à l'objectif d'enquête de la police puisse s'avérer un facteur utile pour démontrer son équivalence sur le plan du fond, l'examen suivant le critère exigeant qu'il n'y ait « aucune disposition » demeure axé sur ce dernier point, non sur le premier. Si la police réussit à démontrer pourquoi l'autorisation qu'elle demande est différente de celles déjà prévues, l'examen fondé sur l'al. 487.01(1)*c*) prend fin.

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

[103] Enfin, deux questions soulevées par le juge Cromwell dans ses motifs méritent d'être clarifiées.

[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.

[104] Premièrement, je ne conclus pas — et je ne voudrais pas non plus laisser entendre — que la police a agi sournoisement ou de mauvaise foi en sollicitant le mandat général en l'espèce. Aucune preuve en ce sens n'a été présentée, et je n'ai aucune raison de croire que la police a agi autrement que de bonne foi. Plus simplement, nous ne savons pas ce qui a motivé la police, et là n'est pas la question. La question de savoir si la police pouvait ou non obtenir une autorisation visée par la partie VI en l'espèce n'est pas pertinente dans la mesure où la condition qu'il n'y ait « aucune disposition » est concernée. Ce qui importe, c'est que nous ne disposons de rien qui puisse aider la police à s'acquitter de son fardeau de démontrer que la technique contestée était *différente sur le plan du fond* d'une interception.

[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.

[105] Deuxièmement, l'approche à laquelle je souscris n'élimine pas la souplesse des enquêtes. Comme l'indiquent clairement les arrêts *Ha* et *Brand*, il s'agit d'un facteur qu'un juge peut examiner lorsqu'il décide si une technique d'enquête est différente sur le plan du fond de sorte qu'un mandat général devrait être décerné. Mais il ne s'agit pas du seul facteur à examiner, et ce facteur doit être abordé avec prudence, particulièrement dans des cas comme celui qui nous occupe, où la délivrance d'un mandat général peut constituer une façon commode pour la police d'éviter la rigidité d'une autre disposition en matière de fouille qui est équivalente sur le plan du fond.

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. (dissenting) —

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

IV. Conclusion

[106] Pour ces motifs, je suis d'avis que la démarche adoptée par la police en l'espèce ne peut être approuvée. Le mandat général est invalide parce que la technique d'enquête qu'il autorisait était équivalente sur le fond à une interception. D'après les faits de l'espèce, le mandat général n'a servi qu'à éviter la rigidité de la partie VI. Comme l'a reconnu le ministère public, la police aurait pu demander une autorisation visée par la partie VI. Cela est suffisant pour trancher le pourvoi et pour conclure qu'elle aurait dû demander une telle autorisation.

[107] Cela dit, bien que nous ne soyons pas en présence d'un tel scénario, je n'irais pas jusqu'à conclure qu'un mandat général ne peut *jamais* autoriser prospectivement la transmission de communications privées futures à la police de façon continue pendant une période prolongée. S'il est convaincu qu'une technique d'enquête précise est différente sur le plan du fond de sorte que les dispositions de la partie VI, ou de toute autre loi, ne prévoient pas la fouille, le juge pourrait décerner le mandat, en supposant que les autres exigences soient respectées. Bien entendu, le juge doit conclure que le mandat « servirait au mieux l'administration de la justice » (al. 487.01(1)*b*)) et « doit » imposer les modalités nécessaires pour que la fouille soit raisonnable dans les circonstances (par. 487.01(3)).

[108] Je suis d'avis d'accueillir le pourvoi et d'annuler le mandat général et l'ordonnance d'assistance connexe.

Version française des motifs de la juge en chef McLachlin et du juge Cromwell rendus par

Le juge Cromwell (dissident) —

I. Aperçu

[109] La Société TELUS Communications (« Telus ») conserve dans ses bases de données une copie de tous les messages textes envoyés ou reçus par ses abonnés. Il s'agit principalement de déterminer en l'espèce si la police doit obtenir une

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

autorisation d'écoute électronique pour obtenir des copies des messages ainsi stockés. Mes collègues, la juge Abella et le juge Moldaver, concluent à la nécessité d'une telle autorisation, bien que pour des motifs très différents. Je ne suis pas de cet avis. Comme le juge de la Cour supérieure de l'Ontario qui a rendu la décision portée en appel, j'estime que l'autorisation d'écoute électronique n'était pas nécessaire. Je rejetterais donc le pourvoi.

II. Faits, historique judiciaire et questions litigieuses

[110] La présente espèce concerne des techniques d'enquête particulières qui peuvent être autorisées sous le régime du *Code criminel*, L.R.C. 1985, ch. C-46, lorsque la police souhaite avoir licitement accès au contenu de messages textes. Avant d'entreprendre l'analyse des questions juridiques précises auxquelles nous sommes confrontés, je donnerai quelques indications techniques au sujet de la messagerie texte et de l'éventail des techniques d'enquête que la police peut employer pour y avoir accès. Je résumerai ensuite brièvement les étapes judiciaires jusqu'au présent pourvoi ainsi que les questions que nous devons trancher.

A. *Le service de messagerie texte de Telus*

[111] Le service de messages courts (« SMC »), communément appelé la messagerie texte, est un service de communication utilisant des protocoles de communication normalisés et des réseaux de téléphonie mobile pour la transmission de courts messages textes entre téléphones cellulaires.

[112] Telus emploie le même système de transmission de messages textes que les autres fournisseurs de services de télécommunications. Lorsqu'un abonné de Telus envoie un message, celui-ci est transmis à une station cellulaire Telus puis acheminé à un centre de commutation mobile, soit l'ordinateur central du réseau Telus. Ce centre de commutation comprend le centre de service de messages courts (« CSMC ») de Telus, qui tente de transmettre le message à son destinataire au moyen de moteurs de routage. Si le destinataire est lui-même un abonné de Telus, le message est envoyé du CSMC à une station cellulaire qui le relaie au

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 two to eight 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

téléphone du destinataire; s'il n'est pas un abonné de Telus, le message est envoyé du CSMC de Telus au CSMC du fournisseur du destinataire puis il est relayé au téléphone du destinataire par une station cellulaire. Lorsque l'appareil du destinataire ne peut recevoir le message (par exemple, s'il est éteint ou s'il n'y a pas de réception), le message texte est conservé au CSMC de Telus pour une période maximale de cinq jours. Si, à l'expiration de cette période, le téléphone du destinataire n'a pu recevoir le message, ce message est effacé. Si un message n'est pas transmis, l'expéditeur n'en est pas informé.

[113] Telus diffère toutefois de la plupart des autres fournisseurs en ce qu'elle conserve pendant au moins 30 jours, dans l'une de ses quatre bases de données, une copie électronique des messages textes passant par son système. Trois bases de données PSMS (la PSMS 1 (base de données principale), la PSMS 2 (base secondaire) et la PSMS 3 (base tertiaire)) reçoivent des messages dans les quinze minutes, environ, suivant leur envoi, et la capacité de chaque base de données détermine dans laquelle de ces bases un message est stocké. Tous les messages textes que reçoit un client de Telus sont copiés, et la copie est expédiée aux bases de données au moment où le téléphone de l'abonné les reçoit du CSMC de Telus. Lorsqu'un abonné de Telus envoie un message texte, le message est copié lorsqu'il arrive au CSMC de Telus, et la copie est stockée dans une base de données. Telus possède en outre une quatrième base de données, appelée PECSMS, qui reçoit des messages dans un délai de deux à huit heures après leur envoi. Au moment de l'instruction de la présente affaire en première instance, Telus prévoyait qu'en avril 2011 la base PECSMS serait l'unique base de stockage des messages textes et l'utilisation des bases PSMS cesserait.

[114] Telus copie les messages textes pour faciliter le dépannage et le traitement des plaintes des clients. Comme je l'expliquerai plus loin, en procédant ainsi, Telus intercepte les messages, ce que le *Code* l'autorise à faire sans autorisation d'écoute électronique. Le but avoué par Telus, jumelé au fait que la plupart des autres fournisseurs

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, that 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)).

de services en Ontario transmettent les messages textes sans en conserver une copie de cette façon, montre clairement, selon moi, que cette étape supplémentaire ne fait pas partie du processus de communication. Le type de stockage en cause ici n'est pas inhérent à la communication de messages textes, contrairement au stockage transitoire des courriels, nécessaire à leur transmission.

B. *Messages textes et techniques d'enquête*

[115] Pour obtenir l'autorisation de prendre connaissance du contenu de messages textes stockés par Telus, la police dispose, en vertu du *Code*, d'au moins trois moyens potentiels : l'ordonnance de communication, le mandat général et l'autorisation d'interception, aussi appelée « autorisation d'écoute électronique ». En l'espèce, la police a demandé et obtenu un mandat général se voulant une sorte d'ordonnance de communication étoffée, mais Telus soutient que la police devait demander une autorisation d'écoute électronique. Les exigences de ces trois techniques d'enquête étant en quelque sorte interreliées, une brève description de chacune sera utile.

1. L'ordonnance de communication

[116] La police peut obtenir le contenu de messages textes stockés en demandant l'ordonnance de communication prévue à l'art. 487.012 du *Code*, lequel énonce qu'un juge de paix ou un juge peut ordonner à une personne « de communiquer des documents — originaux ou copies [. . .] [ou] de préparer un document à partir de documents ou données existants et de le communiquer » (al. 487.012(1)*a*) et *b*)). Les conditions régissant la délivrance d'une ordonnance de communication sont essentiellement les mêmes que pour le mandat de perquisition. Une dénonciation sous serment doit convaincre le juge de paix ou le juge qu'une infraction a été ou est présumée avoir été commise, que les documents ou données fourniront une preuve touchant la perpétration de l'infraction et que ces documents ou données sont en la possession ou à la disposition de la personne visée par l'ordonnance (par. 487.012(3)). En outre, cette personne ne doit pas faire l'objet de l'enquête (par. 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". 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,

[117] Lorsque Telus reçoit signification d'une ordonnance de communication, elle doit communiquer à la police les documents ou données qui sont déjà en sa possession ou des copies de ceux-ci. La police obtient ainsi copie de messages textes qui ont déjà été envoyés ou reçus par les abonnés et stockés dans les bases de données de Telus. On a supposé, et je tiens pour acquis en l'espèce, qu'une ordonnance de communication ne peut viser des documents ou données qui n'existent pas encore (voir les al. 487.012(1)*b*) et 487.012(3)*c*)).

[118] J'ajouterais qu'à première vue, l'art. 487.012 permet à un juge de paix ou un juge d'ordonner la communication de messages textes se trouvant dans les bases de données d'un fournisseur au moyen d'une série d'autorisations quotidiennes. Cet article établit relativement peu de restrictions pour la délivrance d'ordonnances de communication. Contrairement aux autres autorisations examinées en l'espèce, cet article n'exige pas du juge une conclusion que l'ordonnance est nécessaire à l'enquête policière et ne requiert pas que l'ordonnance serve au mieux l'administration de la justice. À l'instar du juge siégeant en révision, je considère que la police aurait pu avoir accès aux messages textes stockés dans les bases de données de Telus au moyen d'une série de telles ordonnances.

2. Le mandat général

[119] Un juge peut décerner un mandat général autorisant un agent de la paix à « utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive » (art. 487.01). Le juge doit être convaincu, par la dénonciation faite sous serment, de l'existence de motifs raisonnables de croire qu'une infraction a été ou sera commise et que l'utilisation de la technique pour laquelle la police demande une autorisation permettra d'obtenir des renseignements au sujet de cette infraction.

[120] Comme une vaste gamme de techniques peuvent être autorisées par un mandat général, le législateur a imposé des conditions supplémentaires

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.

rigoureuses. Premièrement, contrairement aux mandats de perquisition et aux ordonnances de communication qui peuvent émaner de juges ou de juges de paix, le mandat général ne peut être décerné que par un juge (par. 487.01(1)). Deuxièmement, le juge doit être « convaincu que la délivrance du mandat servirait au mieux l'administration de la justice » (al. 487.01(1)*b*)). Troisièmement, le mandat général « doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances » (par. 487.01(3)). Quatrièmement, le mandat général n'est décerné que « s'il n'y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte » (al. 487.01(1)*c*)). Autrement dit, on ne peut avoir recours au mandat général pour autoriser « une telle utilisation ou l'accomplissement d'un tel acte » si d'autres dispositions prévues au *Code* (ou ailleurs) pourraient les autoriser. (Ce que j'appellerai, dans ces motifs, la condition qu'il n'y ait « aucune disposition ».) Telus affirme que cette condition n'était pas respectée parce que les dispositions du *Code* en matière d'écoute électronique prévoient l'autorisation de la technique que la police souhaitait utiliser.

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 or a judge as defined in s. 552 of the *Code*. 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

3. L'autorisation d'écoute électronique

[121] L'autorisation d'intercepter des communications privées délivrée sous le régime de la partie VI du *Code* permet à la police de recevoir les messages au moment où ils sont envoyés ou reçus par les abonnés. Cette autorisation est assujettie à des conditions encore plus strictes que celles qui s'appliquent au mandat général. Elle ne peut être délivrée que par un juge d'une cour supérieure de juridiction criminelle ou par un juge au sens de l'art. 552 du *Code*, et la demande d'autorisation doit être présentée par le procureur général, le ministre de la Sécurité publique et de la Protection civile ou un mandataire spécialement désigné (par. 185(1)). Des dispositions particulières détaillées prévoient ce qui doit être présenté au juge, lequel doit être convaincu non seulement que l'autorisation servirait au mieux l'administration de la justice, mais encore qu'il a été satisfait au critère

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 than 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,

dit de la « nécessité pour l'enquête » (par. 186(1)), ce qui signifie qu'il doit avoir la conviction que « d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête » (par. 186(1)). Généralement, la durée de validité de l'autorisation ne dépasse pas 60 jours (al. 186(4)*e*)), et des exigences en matière d'avis et de rapport s'appliquent (art. 196).

[122] Lorsque l'interception de messages textes est autorisée, Telus installe un dispositif qui achemine automatiquement une copie de chaque message texte à la salle ou au poste d'écoute de la police. Lorsqu'un abonné de Telus envoie un message texte, le dispositif achemine une copie du message lorsque celui-ci arrive au CSMC de Telus. Lorsque l'abonné de Telus reçoit un message texte, l'acheminement de la copie se fait lorsque le message parvient au téléphone de l'abonné. Ainsi, avec l'autorisation d'interception, la police a accès aux messages « en temps réel », dès leur envoi ou leur réception.

C. *Historique judiciaire*

[123] En l'espèce, la police a demandé et obtenu un mandat général ordonnant à Telus de lui fournir copie de messages textes stockés, envoyés et reçus par deux de ses abonnés avant la délivrance du mandat et, aussi, de messages qui seraient envoyés et reçus après la délivrance du mandat, pendant une période d'environ deux semaines. Seule l'autorisation de communication des messages textes postérieurs à la délivrance du mandat est en cause. Relativement à ces derniers messages, Telus devait fournir, au plus tard à 14 h chaque jour, du mardi au vendredi, une copie de tous les messages envoyés ou reçus entre 11 h la veille et 11 h le jour même. Les lundis, elle devait fournir, au plus tard à 14 h, une copie de tous les messages envoyés ou reçus entre 11 h le vendredi précédent et 11 h le lundi. Le mandat général exigeait en outre que Telus fournisse à la police les renseignements relatifs aux abonnés à l'égard de tous les numéros de téléphone avec lesquels les deux abonnés en cause

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

avaient échangé des messages textes. Le mandat général s'apparentait ainsi à une ordonnance de communication, puisqu'il exigeait la communication de copies de messages stockés et de renseignements relatifs aux abonnés s'y rapportant, mais il s'en distinguait du fait qu'il autorisait prospectivement la communication de ces copies.

[124] Telus a demandé l'annulation du mandat général et le juge Sproat a essentiellement rejeté sa demande (2011 ONSC 1143, 105 O.R. (3d) 411). Selon le principal argument invoqué par Telus, le mandat général autorisait une interception, une technique qui pouvait être autorisée sous le régime de la partie VI du *Code*. On ne pouvait donc décerner un mandat général puisque la condition qu'il n'y ait « aucune disposition » permettant cette technique n'avait pas été respectée.

[125] Le juge siégeant en révision a rejeté cet argument. À son avis, le mandat général n'autorisait pas une interception; la police demandait les copies de messages déjà stockés dans les bases de données de Telus; elle ne sollicitait pas l'autorisation d'« intercepter des communications privées ». Le mot « intercepter » exigeait, selon lui, l'obtention en temps réel de communications transitoires, ce qui ne couvrait pas l'obtention de copies de messages stockés dans une base de données. Les dispositions relatives à l'écoute électronique ne pouvaient autoriser que des interceptions et par conséquent, elles n'étaient pas applicables à la technique d'enquête employée par la police en l'espèce. De l'avis du juge siégeant en révision, un mandat général pouvait donc être décerné.

[126] Telus a aussi invoqué d'autres arguments que le juge siégeant en révision a rejetés. Elle a fait valoir que la police aurait dû attendre la fin de la période de 14 jours visée par le mandat général et demander alors une ordonnance unique de communication. Le juge a rejeté cet argument et estimé que la police n'avait pas à attendre si longtemps pour obtenir les messages. Il a ajouté que, bien que la police eût pu demander au juge de paix 14 ordonnances distinctes de communication, cette solution n'était pas pratique dans les circonstances (par. 76). Il a énuméré divers

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

inconvénients liés à l'obligation faite à la police de demander 14 autorisations, dont le fait de devoir répéter quotidiennement la demande, peut-être devant des officiers de justice différents, et les inconvénients en résultant pour Telus, qui devrait donner suite à des mandats quotidiens exigeant une prompte réponse (par. 70). Le juge Sproat a conclu qu'un mandat général unique autorisant la police à recevoir des messages par courriel pendant environ deux semaines était acceptable parce qu'[TRADUCTION] « il n'aurait pas été pratique pour la police d'obtenir chaque jour un mandat pour parvenir au résultat visé par son enquête, soit obtenir pour examen quotidien des messages textes stockés » (par. 76).

[127] Le juge siégeant en révision n'a pas retenu non plus l'argument de Telus voulant que la délivrance du mandat général ne serve pas au mieux l'administration de la justice (al. 487.01(1)*b*)). Il a conclu que la technique pour laquelle l'autorisation était demandée n'était pas une interception. Il a conclu qu'[TRADUCTION] « il n'appartient pas au tribunal de déterminer, pour des considérations d'intérêt public, que le régime législatif est inadéquat et de prendre prétexte de ce qui sert au mieux l'administration de la justice pour élargir en fait la portée de la partie VI du *Code criminel* » (par. 80). Le juge a aussi écarté l'argument de Telus fondé sur la lourdeur et le caractère impraticable du régime du mandat général et le fardeau excessif qu'il imposait, faisant observer que notre Cour avait écarté pareil argument dans *Société Télé-Mobile c. Ontario*, 2008 CSC 12, [2008] 1 R.C.S. 305, par. 60.

D. *Les questions en litige*

[128] Le principal argument avancé devant nous par Telus est que la technique d'enquête autorisée par le mandat général consistait, en fait, en l'interception de communications privées et qu'en vertu de la condition qu'il n'y ait « aucune disposition » prévue à l'al. 487.01(1)*c*), cette technique ne pouvait être autorisée que sous le régime de la partie VI du *Code*. Ma collègue la juge Abella accepte cet argument, mais je ne puis m'y rallier. Mon collègue le juge Moldaver estime pour sa part

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

inutile d'examiner le principal argument de Telus. Selon lui, même si le mandat général ne constitue pas à strictement parler un mandat autorisant une interception, il autorise une technique qui y équivaut fondamentalement et qui, par conséquent, devrait être exclue de l'autorisation par mandat général en application de la condition qu'il n'y ait « aucune disposition » imposée par l'al. 487.01(1)*c*). Deux questions se posent en conséquence :

1. La technique d'enquête autorisée en l'espèce par le mandat général est-elle une interception nécessitant une autorisation sous le régime de la partie VI du *Code*?

2. Si la saisie de messages textes stockés n'est pas une interception, la condition qu'il n'y ait « aucune disposition » énoncée à l'al. 487.01 (1*c*) interdit-elle néanmoins la délivrance d'un mandat général du fait que la technique que l'on demande d'autoriser équivaut fondamentalement à de l'écoute électronique?

III. Analyse

A. *Première question : La technique d'enquête autorisée en l'espèce par le mandat général est-elle une interception nécessitant une autorisation sous le régime de la partie VI du Code?*

[129] Telus plaide qu'un mandat général ne pouvait être décerné en l'espèce car la technique d'enquête que la police cherchait à faire autoriser était l'interception de communications privées. Cette technique d'interception de communications privées peut être autorisée par un juge en vertu de l'art. 186, partie VI, du *Code*. Par conséquent, selon cet argument, le mandat général n'aurait pas dû être décerné parce que la condition qu'il n'y ait « aucune disposition » n'était pas respectée (al. 487.01(1)*c*)).

[130] Ma collègue la juge Abella accepte en gros cet argument. Elle est d'avis que le mandat général était censé autoriser une interception, parce qu'il permettait « la communication *prospective* de futurs messages textes se trouvant dans l'ordinateur

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

d'un fournisseur de services » (par. 15 (en italique dans l'original)). Je crois comprendre que « la communication *prospective* de futurs messages textes » signifie qu'au moment où le mandat est décerné, au moins certains des messages à divulguer n'existent pas encore. J'estime avec égards que ce mandat général n'a pas autorisé une interception.

[131] La technique d'enquête autorisée en l'espèce par le mandat général n'est pas une interception de communications privées qui pourrait être autorisée en vertu de l'art. 186. Le mandat général procure à la police des copies de messages stockés, préalablement interceptés par Telus; la police n'obtient la divulgation des messages que lorsque Telus les récupère de sa base de données et les lui envoie par courriel. La distinction entre la divulgation d'une communication interceptée et l'interception d'une communication, loin d'être une différence « de forme », revêt une importance fondamentale pour ce qui est de l'objet des dispositions relatives à l'écoute électronique et du régime qu'elles établissent.

1. Texte, contexte et régime de la partie VI

[132] La question de savoir si ce que la police a fait en vertu du mandat général constitue l'interception de communications privées relève de l'interprétation de la loi. À mon avis, à la lecture des dispositions législatives dans leur contexte intégral, il est clair que le mandat général ne permet pas une interception nécessitant une autorisation sous le régime de la partie VI.

[133] En règle générale, la police doit obtenir une autorisation pour intercepter une communication privée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre. Les mots clés sont donc « intercepter » et « communication privée ».

[134] La définition du mot « intercepter » n'est pas exhaustive; le terme s'entend notamment du fait « d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet » (art. 183). La définition de l'expression « communication privée » est liée à la notion d'interception. Si

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,

l'on réduit cette définition à l'essentiel, une communication privée est une communication faite « dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers » (art. 183).

[135] Un message texte est incontestablement une communication privée et, comme nous le verrons, il est tout aussi incontestable que Telus a intercepté des messages textes au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre. La question est de savoir si la police a elle aussi intercepté ces messages lorsque Telus lui a remis copie des messages envoyés et reçus qu'elle avait préalablement interceptés et stockés dans ses bases de données.

[136] Cette question m'amène à un examen plus approfondi de l'objet et du texte des dispositions relatives à l'écoute électronique, ainsi que du régime qu'elles établissent. Cet examen permet le mieux, selon moi, de déterminer si le législateur voulait que la technique employée par la police en l'espèce constitue une interception. Les dispositions applicables sont reproduites en annexe.

[137] La distinction entre *l'interception* de communications privées et *la divulgation, l'utilisation ou la conservation* de communications privées qui ont été interceptées est fondamentale pour ce qui est de l'objet des dispositions et du régime qu'elles établissent. L'objet, le texte et le régime de la partie VI montrent que la divulgation, l'utilisation ou la conservation de communications privées interceptées sont distinctes de l'interception elle-même.

[138] Lorsque les dispositions originales en matière d'écoute électronique ont été introduites en 1973, les notes explicatives du projet de loi indiquaient qu'il avait notamment pour but de créer trois types distincts d'infractions. Deux d'entre eux sont pertinents en l'espèce. La première infraction a trait à l'*interception* de communications privées au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre. La seconde a trait à la *divulgation* de communications privées interceptées

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. at the Ontario Court of Appeal) 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. [Emphasis added.]

(*Law of Electronic Surveillance in Canada* (1979), at p. 44)

[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.

de cette façon (Notes explicatives, projet de loi C-176, *Loi sur la protection de la vie privée*, 1re sess., 29e lég. (S.C. 1973-74, ch. 50)). Bien que les notes explicatives fassent moins autorité que l'énoncé des objets figurant dans le texte de loi même, elles peuvent néanmoins donner une idée de l'objectif législatif : R. Sullivan, *Sullivan on the Construction of Statutes* (5e éd. 2008), p. 272. Les notes explicatives indiquent ainsi que, dès le début, le texte de loi avait notamment pour objet de différencier l'interception de communications privées des actes subséquents et distincts que sont la divulgation ou l'utilisation des communications privées interceptées. Cela dénote que le législateur voyait l'interception et la divulgation de communications interceptées comme deux choses différentes et ne voulait donc pas que la divulgation ou l'utilisation de communications interceptées entrent dans la notion d'interception.

[139] Le caractère fondamental de cette distinction pour le régime établi par la loi a été relevé par un des premiers commentateurs de la loi. David Watt (à présent juge à la Cour d'appel de l'Ontario), se demandant si le fait de rejouer, réentendre ou réenregistrer une conversation déjà enregistrée constituait une « interception », a conclu comme suit :

> [TRADUCTION] Le fait de rejouer ou de réentendre la conversation interceptée à l'origine peut fort bien constituer chaque fois une utilisation ou divulgation au sens de l'interdiction applicable, mais utiliser ou divulguer n'est pas nécessairement intercepter, et assimiler les deux revient à faire abstraction de la distinction fondamentale que la loi établit entre ces actes. [Je souligne.]

(*Law of Electronic Surveillance in Canada* (1979), p. 44)

[140] La structure des dispositions de la partie VI créant les infractions reflète cette distinction entre interception et divulgation. En d'autres termes, le texte de loi exprime précisément l'objet énoncé dans les notes explicatives. La partie VI crée des infractions distinctes conformément à l'objet énoncé dans ces notes.

[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

[141] Une infraction, je le répète, interdit l'*interception d'une communication privée*. Selon l'art. 184 du *Code*, « [e]st coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée ». Des exceptions s'appliquent, comme nous le verrons un peu plus loin. L'autre infraction concerne *la divulgation ou l'utilisation des renseignements interceptés*. Aux termes de l'art. 193 du *Code*, commet un acte criminel quiconque utilise ou divulgue le contenu d'une communication privée ou en divulgue l'existence sans le consentement de son auteur ou de la personne à laquelle son auteur la destinait. Là encore, il existe des exceptions et j'y reviendrai. La création de ces deux infractions distinctes souligne que l'acte d'intercepter et l'acte de divulguer ou d'utiliser des communications interceptées sont des actes distincts que le régime établi par la loi traite différemment.

[142] Dans le cas de la première infraction, relative à l'interception, plusieurs « réserves » excluent des actes qui constitueraient par ailleurs une interception illégale. Ces exclusions sont utiles à la compréhension du régime législatif parce qu'elles distinguent *l'interception* de communications de *l'utilisation ou la conservation* des communications interceptées. Sans entrer dans tous les détails, précisons qu'il existe trois catégories d'exonérations de responsabilité criminelle. L'interception d'une communication privée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre ne constitue pas une infraction (i) si l'auteur de la communication ou la personne qui la reçoit y a consenti (al. 184(2)*a*)); (ii) si l'interception est autorisée en conformité des dispositions en cette matière (al. 184(2)*b*)); ou (iii) si l'interception intervient pour la fourniture d'un service de communications ou est faite par un fonctionnaire fédéral chargé de la régulation du spectre des fréquences de radiocommunication ou encore si elle sert à des fins de gestion ou de protection d'un ordinateur (al. 184(2)*c*), *d*) et *e*)).

[143] Ce qui importe est que la troisième réserve — celle qui concerne l'interception en lien avec

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

un ordinateur — distingue *l'interception* de la communication, d'une part, de *l'utilisation* ou de *la conservation* de la communication interceptée, d'autre part. L'alinéa 184(2)*e*) exclut de l'infraction l'interception, par une personne en possession ou responsable d'un ordinateur, de communications privées passant par l'ordinateur lorsque l'interception est raisonnablement nécessaire pour la gestion de la qualité du service de l'ordinateur ou pour la protection de celui-ci. Le paragraphe 184(3), qui repose sur la distinction entre *l'interception* et *l'utilisation ou la conservation*, vient préciser cette exception; une communication privée *interceptée* par une personne en possession ou responsable d'un ordinateur ne peut être *utilisée ou conservée* que si elle est essentielle pour empêcher un dommage à l'ordinateur ou si elle est divulguée conformément à une autre disposition du *Code*.

[144] Ainsi, les dispositions relatives à l'infraction d'interception distinguent l'interception de l'utilisation ou la conservation des communications interceptées, ce qui indique que le législateur y voyait des actes différents et distincts.

[145] Cela nous amène à la deuxième infraction prévue par le régime, qui interdit l'utilisation ou la divulgation de communications privées interceptées. Aux termes du par. 193(1), commet une infraction quiconque *utilise* ou *divulgue* le contenu ou l'existence d'une communication privée interceptée sans qu'il y ait eu consentement. Je signale que l'infraction d'utilisation ou de divulgation concerne « tout ou partie de cette communication privée, ou la substance, le sens ou l'objet de tout ou partie de celle-ci ». L'existence de cette infraction en tant qu'infraction distincte de celle d'interception montre que le législateur considérait l'interception, d'une part, et la divulgation ou l'utilisation, d'autre part, comme des concepts distincts.

[146] La comparaison des exemptions prévues aux art. 184 et 193 me conforte dans cette position. L'article 193 prévoit des exemptions beaucoup plus permissives que celles prévues à l'art. 184, en particulier en ce qui a trait aux enquêtes en matière pénale. Aux termes de l'art. 184, la police ne peut intercepter des communications que si elle est autorisée à le faire (al. 184(2)*b*)) ou dans

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.

certaines circonstances exceptionnelles (art. 184.4). L'article 193, par contre, comprend de larges exemptions qui permettent la divulgation de communications interceptées dans diverses circonstances, notamment lors de poursuites civiles ou pénales (al. 193(2)*a*)) et « au cours ou aux fins d'une enquête en matière pénale » (al. 193(2)*b*)). On peut penser que, si le législateur considérait la divulgation de communications privées interceptées comme une forme d'interception, il y aurait eu une correspondance substantielle entre les exemptions relatives à l'interception et celles qui se rapportent à la divulgation. Or, ce n'est manifestement pas le cas.

[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.

[147] La comparaison des exemptions particulières qui s'appliquent aux fournisseurs de services de communications, énoncées aux par. 193(2) et 184(2), étaye encore plus ce point. On se rappellera que l'interception de communications par les fournisseurs de services de communications ne constitue pas une infraction si elle intervient pour les fins de la fourniture de ces services (al. 184(2)*c*)). Une exception comparable s'applique à l'infraction de divulgation. L'alinéa 193(2)*d*) écarte la responsabilité criminelle à l'égard de la divulgation intervenant dans le cadre de l'exploitation d'un système de communications ou d'un service de gestion ou de protection d'un ordinateur, si la divulgation est nécessairement accessoire aux fins pour lesquelles les exploitants peuvent être exonérés de l'infraction d'interception. Ainsi, les exploitants de systèmes de communications comme Telus jouissent, dans certaines circonstances, d'une exception à l'infraction d'interception et à celle de divulgation. Cela souligne une fois de plus que le législateur considérait ces actes comme distincts.

[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

[148] Pour résumer, le régime législatif crée deux infractions distinctes, l'une qui concerne l'interception, et l'autre, l'utilisation ou la divulgation d'une communication. La distinction entre ces actes est un élément fondamental du régime : si la divulgation ou l'utilisation d'une communication privée en constituait l'interception, il n'aurait pas été nécessaire de les ériger en infraction distincte. De la même façon, les exonérations de responsabilité

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,

criminelle prévues par le législateur indiquent qu'il a établi une distinction entre l'interception, d'une part, et la conservation, l'utilisation et la divulgation, d'autre part.

2. Le mandat général autorisait-il l'interception de communications privées?

[149] Comment cela se rattache-t-il à ce que Telus et la police accomplissaient en vertu du mandat général en l'espèce? S'agissant de Telus, nul ne conteste qu'elle interceptait les messages textes lorsqu'elle les copiait pour les besoins de gestion de ses propres systèmes. Il est pareillement reconnu que Telus n'a pas commis une infraction d'interception illégale (ce que je tiens pour acquis pour le besoin du présent pourvoi). Elle a réalisé des interceptions dans un but autorisé visé par une exonération de responsabilité criminelle. L'alinéa 184(2)*c*) établit clairement que l'interception de communications privées par un fournisseur de services de communications comme Telus ne constitue pas une infraction lorsqu'elle est nécessaire, entre autres choses, pour le contrôle de la qualité des services. Aux termes de l'al. 193(2)*d*), ces fournisseurs peuvent aussi, pour les mêmes besoins, divulguer les communications interceptées sans encourir de responsabilité criminelle. Il ne fait donc aucun doute en l'espèce que Telus a licitement intercepté des communications privées.

[150] Qu'en est-il de ce qu'a fait la police en vertu du mandat général? La police a demandé à Telus la divulgation de renseignements que Telus avait déjà légalement interceptés. Le mandat général n'obligeait pas Telus à intercepter des communications, mais à fournir copie de communications qu'elle avait déjà interceptées à des fins licites qui lui étaient propres. Nul ne prétend que Telus procédait à ces interceptions à la demande de la police; des interceptions effectuées pour des fins policières nécessiteraient clairement une autorisation puisque ces fins ne sont pas visées par l'exception prévue à l'al. 184(2)*c*). Toutefois, comme l'indique clairement le régime législatif, la divulgation ou l'utilisation de communications interceptées légitimement ne constituent pas une interception. J'ai déjà précisé que la partie VI du

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.

Code établit une distinction fondamentale entre *l'interception*, d'une part — c.-à-d. écouter, enregistrer ou prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet — et, d'autre part, *l'utilisation ou la divulgation* d'une communication privée ou de sa substance, son sens ou son objet, ou la divulgation de son existence. La reconnaissance de cette distinction est manifeste dans l'objet des dispositions, dans la création d'infractions distinctes pour l'interception illégale et pour l'utilisation ou la divulgation illégales, ainsi que dans les réserves qui s'appliquent à ces infractions.

[151] À mon avis, la conclusion que la police interceptait des communications privées en recevant de Telus des copies de messages textes déjà interceptés et stockés est incompatible avec la distinction fondamentale qu'établit le texte de loi.

3. Les motifs de la juge Abella

[152] Ce qui m'amène à examiner les motifs de la juge Abella. Selon elle, le mandat général visait à autoriser une interception parce qu'il permettait « la communication *prospective* de futurs messages textes se trouvant dans l'ordinateur d'un fournisseur de services » (par. 15 (en italique dans l'original)); le fait que les messages étaient stockés dans une base de données constitue simplement une différence « technique » propre au mode de prestation de service de Telus qui ne devrait pas priver les abonnés de Telus de la protection du *Code* (par. 3). Par conséquent, la police devait disposer d'une autorisation d'écoute électronique, non d'un mandat général. Cette interprétation s'appuie sur l'inclusion, dans la définition d'« intercepter », des mots « prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet » (art. 183) et sur la nature prospective des autorisations d'écoute électronique. À mon avis, ce raisonnement n'est pas convaincant pour trois raisons.

[153] Le premier problème que j'y vois est qu'il ne donne pas effet à la distinction claire que fait la loi entre l'interception et la divulgation. Pour les

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 electromagnetic, 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

motifs que j'ai déjà exposés, j'estime que l'on ne peut, en la qualifiant de simple « différence technique », rejeter cette distinction, qui constitue un élément fondamental du régime créé par les dispositions en cause. Le législateur a traité l'« interception » et la « divulgation » comme des actes distincts, donnant naissance à des infractions et à des exceptions différentes, même si elles peuvent se rapporter aux mêmes communications privées. Lorsque Telus remet à la police les copies de communications déjà interceptées, elle les divulgue, elle ne les intercepte pas à nouveau. Je ne vois pas comment cette divulgation par Telus de données stockées dans ses bases de données peut constituer une interception par la police.

[154] Le deuxième problème découle de ce que ma collègue s'appuie sur la définition d'« intercepter » énoncée à l'art. 183 et, plus particulièrement, sur le fait qu'« intercepter » inclut « prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet ». Dans son sens large, cette définition d'« intercepter » signifie que chaque fois que la police prend connaissance d'une communication privée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, elle effectue une interception. À mon avis, le contexte et l'objet de la partie VI exigent que les mots « prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet » reçoivent une interprétation plus étroite.

[155] Tout d'abord, le sens des mots « prendre volontairement connaissance » doit être interprété en fonction du contexte où ils s'insèrent; ils font partie d'une énumération comprenant « écouter » et « enregistrer », deux actions se produisant en même temps que l'interception de la communication. Ils servent aussi à expliquer le mot « intercepter », et il est clair, je pense, que beaucoup de façons de prendre volontairement connaissance du contenu d'une communication ne peuvent être considérées comme une interception. De plus, si, comme l'affirme ma collègue la juge Abella (par. 37), « [l]a prise de connaissance de la substance d'une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de

Part VI of the *Code*. Police may well have to obtain a Part VI authorization any time they want access to the content of private communications, no matter when the message has been sent or whether it has 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, [2012] 3 S.C.R. 34, 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 (CanLII), 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

télécommunications » constitue une interception, il se pourrait fort bien alors qu'une autorisation d'écoute électronique soit nécessaire pour une multitude de fouilles ou perquisitions qui ne sont manifestement pas visées par la partie VI du *Code*. La police pourrait devoir obtenir une autorisation sous le régime de cette partie chaque fois qu'elle veut avoir accès au contenu de communications privées, peu importe quand le message a été envoyé ou qu'il ait été reçu ou stocké dans l'appareil du destinataire. Par exemple, selon une interprétation large de « prendre volontairement connaissance », la saisie de courriels d'un appareil BlackBerry constituerait une interception, parce qu'il y a prise de connaissance du contenu de communications privées. De la même façon, une personne autorisée en vertu du par. 487(2.1) à effectuer une perquisition dans un ordinateur aurait besoin d'une autorisation d'écoute électronique pour prendre copie des communications personnelles qui y sont stockées (y compris, par exemple, les courriels et les copies de clavardage). Un tel raisonnement irait à l'encontre du courant jurisprudentiel canadien selon lequel le mandat de perquisition est suffisant pour autoriser l'accès par la police à des documents et données conservés dans un ordinateur : voir, p. ex., *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 73; *R. c. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241, par. 33; *R. c. Bahr*, 2006 ABPC 360, 434 A.R. 1; *R. c. Cross*, 2007 CanLII 64141 (C.S.J. Ont.), par. 25-27; *R. c. Little*, 2009 CanLII 41212 (C.S.J. Ont.), par. 154; *R. c. Tse*, 2008 BCSC 906 (CanLII), par. 198; *R. c. Weir*, 2001 ABCA 181, 281 A.R. 333, par. 19. Si les mots « prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet » recevaient une interprétation large, les communications privées stockées auxquelles la police a depuis longtemps accès au moyen de mandats de perquisition ordinaires seraient visées par la partie VI.

[156] Compte tenu de l'objet des dispositions en matière d'écoute électronique et du régime qu'elles créent, il ne convient pas, à mon avis, d'interpréter de façon aussi large les mots « prendre volontairement connaissance ». Je ne reprendrai pas l'analyse exposée précédemment, sauf à dire qu'il en découle que l'on n'intercepte pas des

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.

communications déjà interceptées et stockées en en prenant connaissance, parce qu'une telle interprétation large est incompatible avec la nette distinction que font les dispositions législatives entre interception et divulgation. L'application générale de cette interprétation de « prendre volontairement connaissance » élargirait bien au-delà de tout ce qui a déjà pu être envisagé le champ des techniques d'enquête nécessitant une autorisation d'écoute électronique.

[157] Ce qui m'amène à traiter l'aspect temporel de la notion d'interception qu'introduit la juge Abella, et c'est la troisième difficulté que me pose son approche. Si je comprends bien, il y a interception si la prise de connaissance du contenu d'une communication privée est autorisée de façon prospective. Par conséquent, la question de savoir si un acte constitue une interception ne dépend pas de la nature de l'acte lui-même ou du moment où il est posé, mais du moment où il est autorisé. Il s'ensuit nécessairement que la saisie de messages textes déjà interceptés et stockés ne constituerait pas une interception dès lors qu'elle était autorisée *après* le stockage des messages. La police pourrait obtenir une ordonnance de communication à la fin de chaque jour pendant la période visée par le mandat général et il n'y aurait pas d'interception. Toutefois, suivant ce critère de l'autorisation prospective, si la police devait saisir les mêmes renseignements, sous la même forme et par les mêmes moyens en vertu d'une autorisation accordée *avant* que les messages ne soient stockés, elle procéderait à une interception. À mon sens, cette conception confond l'acte d'intercepter et la nature de son autorisation.

[158] L'interception est une technique, une façon de prendre connaissance de la substance d'une communication privée. Je ne comprends pas comment la même technique, donnant connaissance de l'information sous la même forme, peut constituer soit une saisie de renseignements stockés, soit une interception, selon le moment où elle est autorisée. C'est pourtant ce à quoi conduit le raisonnement de ma collègue la juge Abella. Je ne puis me rallier à cette conclusion.

4. The 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 to 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.

4. Conclusion relative à la première question

[159] Je suis d'avis que la technique d'enquête que la police était autorisée à employer par le mandat général ne constituait pas une interception au sens des dispositions du *Code* en matière d'écoute électronique.

B. *Deuxième question : Si la saisie de messages textes stockés n'est pas une interception, la condition qu'il n'y ait « aucune disposition » énoncée à l'al. 487.01(1)c) interdit-elle néanmoins la délivrance d'un mandat général du fait que la technique que l'on demande d'autoriser équivaut fondamentalement à de l'écoute électronique?*

[160] Mon collègue le juge Moldaver, comme la juge Abella, annulerait le mandat général au motif que la police n'a pas respecté la condition qu'il n'y ait « aucune disposition », énoncée à l'al. 487.01(1)*c*). Le juge Moldaver parvient toutefois à cette conclusion par un raisonnement différent s'appuyant, si je comprends bien, sur trois points principaux. Premièrement, le mandat général constitue une autorisation qu'il faut utiliser de façon limitée et avec modération (par. 56). Je ne puis accepter ni ce postulat ni le résultat qu'il produit en l'espèce. Deuxièmement, la technique proposée ici par la police équivaut « sur le plan du fond » à une interception et elle ne peut donc être autorisée en vertu du par. 487.01(1) en raison de la condition qu'il n'y ait « aucune disposition », énoncée à l'al. *c*). J'estime respectueusement que le critère de l'« équivalence sur le plan du fond » n'entre pas dans l'analyse relative à l'al. 487.01(1)*c*), et qu'en supposant même qu'il entre dans cette analyse, il ne s'appliquerait pas compte tenu des faits de la présente espèce. Troisièmement, vu cette similarité « sur le plan du fond », le recours au mandat général par la police constitue un « recours abusif » à l'art. 487.01, une « façon commode » pour elle d'éviter la rigidité de l'autorisation d'écoute électronique. Bien que j'estime, comme mon collègue, que les tribunaux doivent veiller à ce que les dispositions relatives au mandat général ne soient pas indûment élargies ou utilisées, ces préoccupations selon moi n'ont pas lieu d'être en l'espèce.

1. The Purpose of the General Warrant Provision

[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* (2nd ed. 2004), 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

1. L'objet des dispositions relatives au mandat général

[161] Le juge Moldaver préconise une interprétation téléologique, et non littérale, de ces dispositions. Je conviens, évidemment, que toutes les lois doivent recevoir une interprétation téléologique, mais je ne partage pas son avis au sujet du résultat de l'interprétation téléologique de ces dispositions.

[162] J'examine d'abord l'objet des dispositions relatives au mandat général. Je ne puis accepter que le par. 487.01(1) ait pour objet de n'accorder l'autorisation prévue que dans des circonstances très restreintes et qu'il faut en conséquence n'y recourir qu'avec « modération ». Au contraire, cette disposition est formulée en termes larges, ainsi que le signalent de nombreux auteurs. Comme l'a indiqué un auteur reconnu :

> [TRADUCTION] En édictant l'art. 487.01 (et l'art. 487.02), le législateur a prévu un pouvoir vaste et complet d'octroi de mandats afin que pratiquement toutes les techniques d'enquête pouvant satisfaire aux conditions posées par *Hunter* en matière d'autorisation judiciaire préalable puissent être autorisées.
>
> (S. C. Hutchison, *Hutchison's Canadian Search Warrant Manual 2005* (2e éd. 2004), p. 143)

Lorsque la Cour d'appel de l'Ontario a examiné cette question dans *R. c. Ha*, 2009 ONCA 340, 96 O.R. (3d) 751, par. 35, autorisation d'appel refusée, [2009] 3 R.C.S. vii, elle s'est refusée à interpréter l'art. 487.01 de façon restrictive. Elle a plutôt confirmé la nature réparatrice de la disposition en citant son arrêt *R. c. Lauda* (1998), 37 O.R. (3d) 513, p. 522-523, conf. par [1998] 2 R.C.S. 683, où elle avait jugé que le mandat général permet une gamme souple de méthodes d'enquête; voir aussi *R. c. Noseworthy* (1997), 33 O.R. (3d) 641, p. 644.

[163] Compte tenu de cette conception de l'objet de l'art. 487.01, j'en aborde l'interprétation différemment de mon collègue. Plus particulièrement, je rejette la prémisse voulant que cet article doive être interprété de façon à en restreindre sévèrement l'utilisation. L'examen porte sur deux points (outre, bien sûr, les motifs raisonnables

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

de croire qu'une infraction a été commise et que l'autorisation demandée permettra d'obtenir des renseignements la concernant) : L'autorisation porte-t-elle sur l'utilisation d'« un dispositif ou une technique ou une méthode d'enquête » ou « l'accomplissement d'un [. . .] acte » prévu par une autre disposition législative fédérale et sert-elle au mieux l'administration de la justice?

[164] Si l'on délaisse l'objet de l'art. 487.01 pour s'attacher plus précisément à l'examen du texte et de l'objet de l'al. 487.01(1)*c*), la disposition ne met pas l'accent sur l'*objectif* d'une enquête mais sur les *moyens* de la réaliser. L'alinéa 487.01(1)*c*) prévoit qu'un mandat général peut être décerné « s'il n'y a aucune disposition [. . .] qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation [d'un dispositif, une technique ou une méthode d'enquête] ou l'accomplissement d'un tel acte ». Les mots « une telle utilisation [d'un dispositif, une technique ou une méthode d'enquête] » et « l'accomplissement d'un tel acte » renvoient tous à *ce que* la police veut faire, non aux *raisons* motivant ce choix. Cet alinéa n'exige pas que le juge saisi examine s'il existe des techniques analogues et si elles permettent d'obtenir les mêmes éléments de preuve, mais simplement si *une telle utilisation* peut être autorisée par une autre disposition.

[165] C'est ce raisonnement que la jurisprudence relative à cette disposition a toujours tenu, et c'est ce qu'a affirmé le juge MacPherson, dans *Ha*, lorsqu'il a indiqué ce qui suit, au par. 43 :

> [TRADUCTION] L'analyse relative à l'al. 487.01(1)*c*) ne porte pas sur l'existence d'autres techniques d'enquête qui pourraient répondre aux besoins ou aux objectifs d'enquête de la police; elle porte plutôt sur la technique ou méthode d'enquête particulière que la police cherche à utiliser et sur la possibilité que cette utilisation puisse être autorisée par une autre disposition. [Je souligne.]

Il ne s'agit pas simplement d'une interprétation étroite et littérale de l'art. 487.01. Il s'agit plutôt d'une interprétation qui rend compte de son objet : l'octroi au juge du vaste pouvoir discrétionnaire d'autoriser la police « à utiliser un dispositif ou une technique ou une méthode d'enquête, ou à

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

accomplir tout acte », pourvu, naturellement, que le juge soit convaincu que l'autorisation sert au mieux l'administration de la justice après avoir accordé l'importance voulue à la protection constitutionnelle contre les fouilles, perquisitions et saisies abusives. Je souscris entièrement à l'opinion du juge MacPherson, qui rendait le jugement de la Cour d'appel de l'Ontario dans *Ha*, lorsqu'il écrit qu'il ne voit [TRADUCTION] « aucune raison de principe justifiant que l'on s'acharne à restreindre la portée de l'art. 487.01 en y ajoutant des mots que le législateur n'y a pas expressément employés » (par. 37).

[166] Je constate que le juge Moldaver s'appuie sur le même paragraphe de l'arrêt *Ha* pour affirmer que les objectifs d'enquête interviennent dans l'analyse relative à l'al. 487.01(1)*c*), sous-entendant que, dans ce passage, le juge MacPherson a adopté une approche qui prend en compte les différences « de fond » entre les diverses techniques (par. 70). Lorsqu'on les considère dans leur intégralité, toutefois, les motifs du juge MacPherson n'appuient pas une telle affirmation. Le juge MacPherson, à mon sens, n'« expliqu[ait] [pas] en quoi la fouille autorisée [. . .] dans l'arrêt *Ha* était différente, sur le plan du fond, d'une fouille nécessitant plusieurs mandats ordinaires » (le juge Moldaver, par. 70). Cela ressort clairement non seulement du passage du paragraphe que j'ai cité précédemment, mais aussi de la façon dont le juge MacPherson résume sa conclusion au par. 41 : [TRADUCTION] « Il n'existe tout simplement aucune disposition [. . .] permettant d'autoriser un nombre illimité d'entrées et de fouilles clandestines dans une propriété privée pour une période de deux mois. » Le juge MacPherson a simplement comparé, dans son analyse relative à l'al. 487.01(1)*c*), la fouille ou perquisition pour laquelle la police demandait un mandat général avec d'autres dispositions en matière de fouilles et perquisitions, et il a conclu qu'aucune de ces dispositions n'autoriserait ce que la police cherchait à faire.

[167] De la même façon, le juge Frankel, rendant jugement pour la cour dans *R. c. Brand*, 2008 BCCA 94, 229 C.C.C. (3d) 443 (*sub nom. R. c. Ford*), par. 50, a déclaré que [TRADUCTION] « [l]e

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.

recours à un mandat général n'est interdit que lorsque l'autorisation judiciaire de l'"utilisation" proposée ou l'"accomplissement d'un tel acte" pourrait être obtenue aux termes d'une autre disposition législative fédérale. » On ne trouve nulle part dans ses motifs d'indication qu'une analyse de l'équivalence fondamentale ou de la nécessité pour l'enquête est requise.

[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

[168] La comparaison de l'al. 487.01(1)*c*) avec l'al. 186(1)*b*), qui énonce l'exigence en matière de nécessité pour l'enquête à laquelle il faut satisfaire pour que l'écoute électronique soit autorisée, me conforte dans mon interprétation. Selon l'al. 186(1)*b*), l'autorisation visée ne peut être donnée que si le juge est convaincu que

> 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.

> d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête.

In *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 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).

Dans *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992, la Cour a posé qu'aux termes de l'al. 186(1)*b*), l'autorisation d'écoute électronique ne peut être accordée que si le juge est convaincu que « [s]ur le plan pratique » il n'existe « aucune autre méthode d'enquête raisonnable, dans les circonstances de l'enquête criminelle considérée » (par. 29 (soulignement omis)). Le législateur a prévu ici une norme élevée; il ne suffit pas que l'interception soit « plus efficace » que d'autres techniques utilisables, elle doit être *nécessaire* à l'enquête (*Araujo*, par. 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*).

[169] L'alinéa 487.01(1)*c*), par contre, exige uniquement que le juge soit convaincu qu'aucune disposition du *Code* ou d'une autre loi fédérale ne peut autoriser la technique envisagée. Il n'a pas à être convaincu en outre que la technique nouvelle est nécessaire à l'enquête ou qu'elle n'est pas équivalente sur le plan du fond à un procédé pouvant être autorisé par une autre disposition. Le législateur savait comment exiger que le juge examine la question de savoir si d'autres techniques d'enquête permettraient d'atteindre le but visé par l'enquête. Il l'a fait à l'al. 186(1)*b*). Mais il ne l'a pas fait à l'al. 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

[170] Évidemment, cela ne veut pas dire qu'un juge devrait autoriser tout ce que la police cherche à faire simplement parce que l'autorisation n'est pas prévue par un autre texte législatif. Son pouvoir discrétionnaire de décerner le mandat doit s'exercer en donnant pleinement effet à la protection des attentes raisonnables en matière de vie privée, comme l'établit l'abondante jurisprudence relative à l'art. 8 de la *Charte canadienne des droits et libertés*. L'exercice de ce pouvoir discrétionnaire du juge ne doit pas permettre à la police de recourir au mandat général pour échapper aux exigences en matière d'autorisation préalable que le législateur a imposées à l'égard de certaines techniques d'enquête. Ainsi que je vais l'expliquer, toutefois, j'estime que, lorsque la question surgit, elle relève directement et expressément de l'al. 487.01(1)*b*), non de l'al. 487.01(1)*c*) auquel on aurait ajouté par interprétation une restriction qui n'y est pas prévue.

[171] Pour résumer ce point, l'inclusion à l'al. 487.01(1)*c*) d'un critère de « l'équivalent sur le plan du fond » n'est étayée ni par le texte de cette disposition, ni par son objet, ni par la jurisprudence. La question posée par cet alinéa est simple : Est-ce qu'une loi fédérale prévoit « un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte »? Lorsque cette condition préalable est respectée, le juge peut envisager d'accorder l'autorisation demandée. La question de savoir *s'il y a lieu* d'accorder l'autorisation demandée ne relève pas de cet alinéa. Ainsi que je l'expliquerai, pour déterminer s'il y a lieu de décerner un mandat général, il faut plutôt se tourner vers l'al. 487.01(1)*b*), lequel pose la question de savoir si la délivrance du mandat général servirait au mieux l'administration de la justice. J'estime que le texte et l'objet de la disposition de même que la jurisprudence étayent une telle approche, alors que celle que propose le juge Moldaver engendre aussi une incertitude inutile et détourne le juge de la question de la compatibilité de la technique visée par la demande d'autorisation avec le droit à la protection contre les fouilles, perquisitions et saisies abusives.

[172] Abordons en premier lieu la question de l'incertitude. J'estime que la prévisibilité et la

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.

clarté du droit revêtent une importance particulière en matière d'autorisation judiciaire préalable de fouilles et de perquisitions. L'autorisation judiciaire préalable est un pilier de la protection garantie par la *Charte* contre les fouilles, perquisitions et saisies abusives. L'autorisation préalable n'a pas pour but premier de détecter après le fait des fouilles ou perquisitions abusives, mais d'en prévenir l'existence. Les exigences en matière d'autorisation préalable doivent être aussi claires que possible pour assurer l'entière protection du droit garanti par la *Charte*.

[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.

[173] La clarté sert également un important objectif pratique. Contrairement à ce qui s'est produit en l'espèce, la contestation de l'autorisation préalable intervient généralement après le fait, lors du procès. Si elle est accueillie, elle compromet l'admissibilité de la preuve obtenue grâce à la fouille ou la perquisition autorisée. La police ne peut remédier après le fait à l'utilisation d'un procédé d'enquête dont l'autorisation est par la suite jugée viciée. C'est pourquoi la clarté du droit revêt une grande importance pratique pour les juges et juges de paix appelés à autoriser des fouilles ou perquisitions et pour les policiers qui demandent ces autorisations.

[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.

[174] Je vois de sérieuses lacunes à cet égard dans l'interprétation retenue par mon collègue le juge Moldaver. Celle-ci ne permet pas de déterminer quand une technique d'enquête équivaut fondamentalement à une autre et quand les différences touchent simplement la forme. Comme il en sera question dans la section suivante de mes motifs, l'application que fait mon collègue du critère de l'« équivalent sur le plan du fond » en l'espèce illustre cette incertitude.

[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

[175] J'estime en outre que cette interprétation de l'al. 487.01(1)*c*) n'aidera pas les juges saisis de demandes d'autorisation à donner effet à la protection contre les fouilles, perquisitions et saisies abusives garantie par la Constitution. Cette question doit s'examiner directement en fonction de l'al. 487.01(1)*b*), non par l'appréciation du degré de ressemblance entre deux techniques au moyen d'un exercice comparatif vague, inutile et en grande partie sémantique. Comme je l'exposerai,

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 nor 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.

même lorsqu'on aborde directement la question en l'espèce, les arguments invoqués à l'encontre de l'autorisation du mandat général, à mon humble avis, ne convainquent pas.

2. La technique proposée est-elle « l'équivalent sur le plan du fond » de l'interception?

[176] Même si j'admettais (et ce n'est pas le cas) que l'al. 487.01(1)*c*) comporte une idée d'équivalence fondamentale de diverses techniques d'enquête, je ne conclurais pas que la technique visée par la demande d'autorisation en l'espèce équivaut fondamentalement à l'autorisation d'écoute électronique. Mon collègue le juge Moldaver est d'avis que le mandat général autorisait en l'espèce une technique constituant au fond une interception « car il permet *prospectivement* à la police d'accéder à des communications privées *futures* de façon *continue* pendant une période prolongée » et que, « [a]bstraction faite du délai de 24 heures, les techniques d'enquête étaient les mêmes » (par. 61 et 68 (en italique dans l'original)).

[177] J'estime avec égards que cette affirmation n'est ni étayée par les faits ni conforme au droit.

[178] S'agissant d'abord des faits, l'autorisation d'écoute électronique seule ne permettrait pas à la police d'obtenir les renseignements que Telus devait fournir en exécution du mandat général. D'ailleurs, la preuve soumise par Telus montre qu'il faudrait trois autorisations distinctes pour que la police ait accès à l'information qu'elle recevrait grâce au mandat général. Comme je l'ai expliqué précédemment, lorsque Telus donne suite à une autorisation d'écoute électronique, elle installe un dispositif qui réachemine en temps réel à la police une copie de tout message texte envoyé ou reçu par un numéro particulier. En l'espèce, le mandat général obligeait Telus à faire plus : elle devait extraire de ses bases de données des messages textes qui y étaient stockés et fournir, avec eux, les renseignements relatifs à l'abonné qui s'y rapportaient.

[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.

[179] Dans l'affidavit qu'elle a déposé devant le juge siégeant en révision, une analyste en sécurité chez Telus, Corinne McNish a indiqué que trois autorisations différentes seraient nécessaires pour obtenir les renseignements demandés en vertu du mandat général : une autorisation prévue au par. 492.2(1) pour placer un téléphone sous enregistreur de numéros, une autorisation prévue au par. 492.2(2) pour obtenir des registres de téléphone, et une autorisation visée à la partie VI. J'ajouterais que, pour tirer parti d'une autorisation relevant de la partie VI, la police doit disposer d'une salle ou d'un poste d'écoute pour la réception des messages et affecter des agents au traitement de l'information entrante, au traitement des renseignements obtenus de l'enregistreur de numéros de téléphone et à l'examen des registres de téléphone.

[180] Compte tenu de la preuve soumise par Telus elle-même, il me semble plutôt exagéré d'affirmer que les techniques d'enquête étaient fondamentalement les mêmes.

[181] En dépit de ces différences claires et importantes entre les deux techniques, mon collègue conclut à leur équivalence fondamentale en s'appuyant largement sur deux faits : le fait qu'en vertu du mandat général, l'accès de la police aux renseignements n'était décalé que de 24 heures, et le fait que le mandat général autorisait « prospectivement » la transmission des messages stockés. Selon moi, le premier fait est inexact, et le second n'étaye pas la conclusion qui en est tirée.

[182] Pour ce qui est du délai, mon collègue estime que le temps écoulé entre le moment où les messages étaient envoyés et celui où la police devait les recevoir était si court que leur communication équivalait, sur le plan du fond, à une interception. Bien qu'il se refuse à indiquer combien de temps devrait s'écouler avant que la technique se différencie, sur le plan du fond, d'une interception, il conclut que « l'intervalle de 24 heures en l'espèce était insuffisant » (note de bas de page 2). Je ne suis pas d'accord avec lui pour deux raisons.

[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, 2010, and end on April 16, 2010. 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*).

[183] Premièrement, comme le mandat général lui-même l'indique clairement, la réception de certains messages qui devaient être remis à la police pouvait être décalée de 72 heures, non de 24 heures. La communication ordonnée par le mandat général devait débuter le 30 mars 2010 et prendre fin le 16 avril de la même année. Le mardi 30 mars, Telus devait communiquer les renseignements se rapportant à la période du 18 au 30 mars, et le ministère public reconnaît que ces renseignements, qui pouvaient s'obtenir au moyen d'une ordonnance de communication, ne pouvaient faire l'objet d'un mandat général. Relativement aux deux semaines et demie subséquentes, le mandat général créait deux intervalles différents, ainsi que je l'ai déjà indiqué. Du mardi au vendredi, Telus devait fournir chaque jour, à 14 h au plus tard, les messages envoyés et reçus entre 11 h la veille et 11 h le jour en cause. Pendant les week-ends, toutefois, l'« intervalle » s'allongeait; les lundis, Telus devait fournir à 14 h au plus tard les messages stockés entre 11 h le vendredi précédent et 11 h le lundi. Ainsi, il y a eu 12 jours où la communication a été quotidienne, mais pour les six jours visés par le mandat général qui tombaient pendant un week-end, l'« intervalle » passait à 72 heures. Il faut donc se demander si ce délai de 72 heures « était insuffisant » lui aussi et, s'il ne l'était pas, si la police aurait eu besoin d'autorisations différentes pour les messages qu'elle recevait le lundi et pour ceux qu'elle recevait les autres jours de la semaine.

[184] Deuxièmement, parce que je partage l'avis du juge siégeant en révision selon lequel la police aurait pu obtenir une série d'ordonnances de communication quotidiennes, il m'est difficile d'accepter que l'« intervalle » de 24 heures sur lequel s'appuie le juge Moldaver fait du mandat général l'équivalent, sur le plan du fond, d'une interception. Une telle série d'ordonnances aurait fourni à la police des copies des messages textes dans les 24 heures suivant leur envoi. Compte tenu de ce qui est, sur le plan du fond, une interception, selon mon collègue, certaines ordonnances de communication pourraient donc équivaloir elles aussi à des interceptions. Cela fait ressortir, selon moi, la confusion et l'incertitude inhérentes à l'application du concept d'équivalence à l'al. 487.01(1)*c*) sur le plan du fond.

[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.

[185] Le deuxième fait sur lequel repose la conclusion d'équivalence sur le plan du fond est la nature « prospective » de l'autorisation. Comme je l'ai déjà indiqué, toutefois, on comprend difficilement de quelle façon, exactement, une même technique peut ou non équivaloir à une interception selon le moment où elle est autorisée. Si, pour les besoins du présent pourvoi, nous reconnaissons — ce que je fais — que la police pouvait légalement obtenir des ordonnances quotidiennes de communication, il est tout simplement incompréhensible que le fait d'autoriser cette technique deux semaines plus tôt convertisse l'ordonnance de communication en une autorisation d'écoute électronique.

[186] Enfin, la conclusion d'équivalence sur le plan du fond est incompatible avec le texte des dispositions relatives à l'écoute électronique et le régime qu'elles établissent. Comme je l'ai déjà expliqué en détail, la divulgation de communications privées déjà interceptées est considérée et traitée, au *Code*, comme un acte distinct de l'interception elle-même. Je ne puis donc voir une simple différence de forme dans une distinction à laquelle le législateur a attaché valeur juridique.

[187] En résumé, je suis d'avis que, même si l'on acceptait l'ajout par interprétation, à l'al. 487.01(1)*c*), d'un critère de « l'équivalent sur le plan du fond », ni les faits ni le droit n'étayent son application en l'espèce.

[188] Cela souligne aussi, selon moi, la confusion et l'incertitude qu'engendrerait l'adoption d'un tel critère. Mon collègue ne fournit aucune indication utile sur ce point, exception faite de celle qui concerne l'« intervalle » de 24 heures, qui est d'ailleurs problématique parce qu'elle entre en conflit avec la possibilité d'obtenir des ordonnances quotidiennes de communication en vertu de l'art. 487.012. À mon avis, il ne faut pas laisser aux juges saisis de demandes d'autorisation et aux enquêteurs de la police le soin de tirer eux-mêmes la ligne en espérant, sans avoir beaucoup de motifs d'optimisme, qu'à l'issue d'un voir-dire on leur donnera raison au procès.

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, e.g., 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".

3. Le recours abusif au mandat général

[189] Nous en arrivons au véritable nœud de la question : Fallait-il refuser de décerner le mandat général parce qu'il constituait, comme le laisse entendre mon collègue, un « recours abusif » à l'art. 487.01, une « solution facile », une « façon commode », un « moyen », ou un « moyen détourné » qui permet à la police « de contourner les exigences » de la partie VI (par. 72, 81, 90 et 105)? D'après ce que je comprends des motifs du juge Moldaver, il arrive à cette interprétation de l'al. 487.01(1)*c*) en raison de la nécessité d'empêcher l'exercice abusif du pouvoir de décerner un mandat général. J'admets que le juge saisi d'une demande de mandat général doit veiller à ce que toute technique d'enquête autorisée respecte entièrement le droit à la protection contre les fouilles, perquisitions et saisies abusives. Toutefois, j'estime que cette analyse doit relever directement de l'al. 487.01(1)*b*), et non passer par le prisme d'une interrogation sur l'équivalence de deux techniques sur le plan du fond.

[190] Comme le juge MacPherson l'a judicieusement fait remarquer dans *Ha*, la condition énoncée à l'al. 487.01(1)*c*) qu'il n'y ait « aucune disposition » n'est pas la seule qui doive être respectée pour qu'un mandat général soit décerné (par. 44). Il ne faut pas aborder cet article en supposant que le législateur voulait que chaque technique d'enquête non autorisée ailleurs puisse être autorisée en vertu du par. 487.01(1) : voir, p. ex., S. Coughlan, « *R. v. Ha* : Upholding General Warrants without Asking the Right Questions » (2009), 65 C.R. (6th) 41. Il faut plutôt que le juge saisi de la demande de mandat soit également convaincu que l'autorisation de la technique en cause sert au mieux l'administration de la justice (al. 487.01(1)*b*)). Selon moi, c'est sous l'autorité de cette disposition que s'examine la question des recours potentiellement abusifs au mandat général. Naturellement, même lorsque les conditions énoncées aux al. 487.01(1)*b*) et *c*) sont respectées, il faut, conformément au par. 487.01(3), que le mandat général énonce « les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances ».

[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 wire room, 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.

[191] L'alinéa 487.01(1)*b*) n'a pas été invoqué dans le présent pourvoi et je ne veux pas le commenter longuement, sauf pour dire qu'il s'agit, à mon avis, de la partie de l'art. 487.01 qui permet d'aborder les préoccupations liées à l'opportunité d'autoriser une nouvelle technique d'enquête. Cela dit, j'estime que les préoccupations évoquées par le juge Moldaver lorsqu'il propose le critère de l'« équivalent sur le plan du fond » ne sont pas du tout convaincantes.

[192] Premièrement, je ne suis pas prêt à conclure que la demande de la police visant à obtenir un mandat général en l'espèce était une « façon commode » de contourner les exigences de la partie VI. Bien entendu, cela n'a pas été prouvé. Deuxièmement, je ne souscris pas à l'affirmation que les droits à la vie privée qui sont en jeu en l'espèce et lors d'une demande d'autorisation d'écoute électronique sont exactement les mêmes. Le juge siégeant en révision a estimé que des ordonnances de communication quotidiennes pouvaient être accordées pour permettre à la police d'obtenir des copies de messages stockés, et je suis d'accord avec lui. Je ne vois pas comment les droits au respect de la vie privée en cause diffèrent si l'autorisation de procéder ainsi est donnée deux semaines à l'avance. Troisièmement, pour tous les motifs formulés par le juge siégeant en révision, il était plus pratique de recourir au mandat général que de demander une série d'ordonnances de communication. Quatrièmement, le mandat général a autorisé une technique qui, outre qu'elle différait d'une interception, répondait mieux aux besoins de la police. Plus particulièrement, elle était beaucoup moins onéreuse en termes de ressources policières, du fait qu'elle n'obligeait pas la police à affecter du personnel à une salle d'écoute et à extraire les renseignements des registres d'abonnés et des enregistreurs de numéros. À mon avis, le mandat général permettait l'atteinte des objectifs légitimes de l'enquête policière de façon beaucoup plus pratique et économique que ce qui aurait pu être autorisé en vertu de toute autre disposition.

[193] Bien sûr, le mandat général avait pour effet de transférer les coûts à Telus. Cependant, cela n'a rien à voir avec le droit à la vie privée des

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;

. . .

abonnés. Qui plus est, le juge siégeant en révision a catégoriquement rejeté la preuve et les arguments de Telus se rapportant au fardeau que le mandat général lui imposait, et Telus ne les a pas présentés devant nous.

[194] Dans le dossier qui nous a été soumis, je ne vois pas de preuve de « recours abusif » à l'art. 487.01 ou de tentative par la police de « contourner les exigences » de la partie VI. Je constate plutôt qu'un service de police municipal de taille plutôt réduite a mené une enquête de façon efficace et pratique, en respectant pleinement le droit à la vie privée des personnes visées par l'enquête ainsi que des autres abonnés de Telus.

C. *Conclusion*

[195] Pour ces motifs, je suis d'avis que le mandat général n'a pas autorisé une interception nécessitant une autorisation d'écoute électronique sous le régime de la partie VI et que la condition qu'il n'y ait « aucune disposition », énoncée à l'al. 487.01(1)*c*), a été respectée.

IV. Dispositif

[196] Je suis d'avis de rejeter le pourvoi.

ANNEXE

Code criminel, L.R.C. 1985, ch. C-46

PARTIE VI

ATTEINTES À LA VIE PRIVÉE

183. Les définitions qui suivent s'appliquent à la présente partie.

. . .

« communication privée » Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition

"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 electromagnetic, 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;

vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

. . .

« intercepter » S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet.

. . .

184. (1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée.

(2) Le paragraphe (1) ne s'applique pas aux personnes suivantes :

a) une personne qui a obtenu, de l'auteur de la communication privée ou de la personne à laquelle son auteur la destine, son consentement exprès ou tacite à l'interception;

b) une personne qui intercepte une communication privée en conformité avec une autorisation ou en vertu de l'article 184.4, ou une personne qui, de bonne foi, aide de quelque façon une autre personne qu'elle croit, en se fondant sur des motifs raisonnables, agir en conformité avec une telle autorisation ou en vertu de cet article;

c) une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans l'un ou l'autre des cas suivants :

(i) cette interception est nécessaire pour la fourniture de ce service,

(ii) à l'occasion de la surveillance du service ou d'un contrôle au hasard nécessaire pour les vérifications mécaniques ou la vérification de la qualité du service,

(iii) cette interception est nécessaire pour protéger ses droits ou biens directement liés à la fourniture d'un service de communications téléphoniques, télégraphiques ou autres;

(*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

d) un fonctionnaire ou un préposé de Sa Majesté du chef du Canada chargé de la régulation du spectre des fréquences de radiocommunication, pour une communication privée qu'il a interceptée en vue d'identifier, d'isoler ou d'empêcher l'utilisation non autorisée ou importune d'une fréquence ou d'une transmission;

e) une personne — ou toute personne agissant pour son compte — qui, étant en possession ou responsable d'un ordinateur — au sens du paragraphe 342.1(2) —, intercepte des communications privées qui sont destinées à celui-ci, en proviennent ou passent par lui, si l'interception est raisonnablement nécessaire :

(i) soit pour la gestion de la qualité du service de l'ordinateur en ce qui concerne les facteurs de qualité tels que la réactivité et la capacité de l'ordinateur ainsi que l'intégrité et la disponibilité de celui-ci et des données,

(ii) soit pour la protection de l'ordinateur contre tout acte qui constituerait une infraction aux paragraphes 342.1(1) ou 430(1.1).

(3) La communication privée interceptée par la personne visée à l'alinéa (2)*e*) ne peut être utilisée ou conservée que si, selon le cas :

a) elle est essentielle pour détecter, isoler ou empêcher des activités dommageables pour l'ordinateur;

b) elle sera divulguée dans un cas visé au paragraphe 193(2).

. . .

185. (1) Pour l'obtention d'une autorisation visée à l'article 186, une demande est présentée *ex parte* et par écrit à un juge d'une cour supérieure de juridiction criminelle, ou à un juge au sens de l'article 552, et est signée par le procureur général de la province ou par le ministre de la Sécurité publique et de la Protection civile ou par un mandataire spécialement désigné par écrit pour l'application du présent article par :

a) le ministre lui-même ou le sous-ministre de la Sécurité publique et de la Protection civile lui-même, si l'infraction faisant l'objet de l'enquête est une infraction pour laquelle des poursuites peuvent, le cas échéant, être engagées sur l'instance du gouvernement du Canada et conduites par le procureur général du Canada ou en son nom;

(*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.

. . .

b) le procureur général d'une province lui-même ou le sous-procureur général d'une province lui-même, dans les autres cas;

il doit y être joint un affidavit d'un agent de la paix ou d'un fonctionnaire public pouvant être fait sur la foi de renseignements tenus pour véridiques et indiquant ce qui suit :

c) les faits sur lesquels le déclarant se fonde pour justifier qu'à son avis il y a lieu d'accorder une autorisation, ainsi que les détails relatifs à l'infraction;

d) le genre de communication privée que l'on se propose d'intercepter;

e) les noms, adresses et professions, s'ils sont connus, de toutes les personnes dont les communications privées devraient être interceptées du fait qu'on a des motifs raisonnables de croire que cette interception pourra être utile à l'enquête relative à l'infraction et une description générale de la nature et de la situation du lieu, s'il est connu, où l'on se propose d'intercepter des communications privées et une description générale de la façon dont on se propose de procéder à cette interception;

. . .

h) si d'autres méthodes d'enquête ont ou non été essayées, si elles ont ou non échoué, ou pourquoi elles paraissent avoir peu de chance de succès, ou si, étant donné l'urgence de l'affaire, il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête.

. . .

186. (1) Une autorisation visée au présent article peut être donnée si le juge auquel la demande est présentée est convaincu que :

a) d'une part, l'octroi de cette autorisation servirait au mieux l'administration de la justice;

b) d'autre part, d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête.

. . .

(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

(4) Une autorisation doit :

a) indiquer l'infraction relativement à laquelle des communications privées pourront être interceptées;

b) indiquer le genre de communication privée qui pourra être interceptée;

c) indiquer, si elle est connue, l'identité des personnes dont les communications privées doivent être interceptées et donner une description générale du lieu où les communications privées pourront être interceptées, s'il est possible de donner une description générale de ce lieu, et une description générale de la façon dont les communications pourront être interceptées;

d) énoncer les modalités que le juge estime opportunes dans l'intérêt public;

e) être valide pour la période maximale de soixante jours qui y est indiquée.

. . .

193. (1) Lorsqu'une communication privée a été interceptée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre sans le consentement, exprès ou tacite, de son auteur ou de la personne à laquelle son auteur la destinait, quiconque, selon le cas :

a) utilise ou divulgue volontairement tout ou partie de cette communication privée, ou la substance, le sens ou l'objet de tout ou partie de celle-ci;

b) en divulgue volontairement l'existence,

sans le consentement exprès de son auteur ou de la personne à laquelle son auteur la destinait, est coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans.

(2) Le paragraphe (1) ne s'applique pas à une personne qui divulgue soit tout ou partie d'une communication privée, ou la substance, le sens ou l'objet de tout ou partie de celle-ci, soit l'existence d'une communication privée :

a) au cours ou aux fins d'une déposition lors de poursuites civiles ou pénales ou de toutes autres

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

procédures dans lesquelles elle peut être requise de déposer sous serment;

b) au cours ou aux fins d'une enquête en matière pénale, si la communication privée a été interceptée légalement;

c) en donnant le préavis visé à l'article 189 ou en fournissant des détails complémentaires en application d'une ordonnance rendue en vertu de l'article 190;

d) au cours de l'exploitation :

(i) soit d'un service de communications téléphoniques, télégraphiques ou autres à l'usage du public,

(ii) soit d'un ministère ou organisme du gouvernement du Canada,

(iii) soit d'un service de gestion ou de protection d'un ordinateur — au sens du paragraphe 342.1(2) —,

si la divulgation est nécessairement accessoire à une interception visée aux alinéas 184(2)*c*), *d*) ou *e*);

e) lorsque la divulgation est faite à un agent de la paix ou à un poursuivant au Canada ou à une personne ou un organisme étranger chargé de la recherche ou de la poursuite des infractions et vise à servir l'administration de la justice au Canada ou ailleurs;

f) lorsque la divulgation est faite au directeur du Service canadien du renseignement de sécurité ou à un employé du Service et vise à permettre au Service d'exercer les fonctions qui lui sont conférées en vertu de l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*.

. . .

PARTIE XV

PROCÉDURE ET POUVOIRS SPÉCIAUX

. . .

487. (1) Un juge de paix qui est convaincu, à la suite d'une dénonciation faite sous serment selon la formule 1, qu'il existe des motifs raisonnables de croire que, dans un bâtiment, contenant ou lieu, se trouve, selon le cas :

(*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;

a) une chose à l'égard de laquelle une infraction à la présente loi, ou à toute autre loi fédérale, a été commise ou est présumée avoir été commise;

b) une chose dont on a des motifs raisonnables de croire qu'elle fournira une preuve touchant la commission d'une infraction ou révélera l'endroit où se trouve la personne qui est présumée avoir commis une infraction à la présente loi, ou à toute autre loi fédérale;

c) une chose dont on a des motifs raisonnables de croire qu'elle est destinée à servir aux fins de la perpétration d'une infraction contre la personne, pour laquelle un individu peut être arrêté sans mandat;

c.1) un bien infractionnel,

peut à tout moment décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

d) d'une part, à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir;

e) d'autre part, sous réserve de toute autre loi fédérale, dans les plus brefs délais possible, à transporter la chose devant le juge de paix ou un autre juge de paix de la même circonscription territoriale ou en faire rapport, en conformité avec l'article 489.1.

(2) Lorsque le bâtiment, contenant ou lieu est situé dans une autre circonscription territoriale, le juge de paix peut délivrer son mandat dans la même forme, modifiée selon les circonstances, et celui-ci peut être exécuté dans l'autre circonscription territoriale après avoir été visé, selon la formule 28, par un juge de paix ayant juridiction dans cette circonscription; le visa est apposé sur l'original du mandat ou sur une copie transmise à l'aide d'un moyen de télécommunication.

(2.1) La personne autorisée à perquisitionner des données contenues dans un ordinateur se trouvant dans un lieu ou un bâtiment peut :

a) utiliser ou faire utiliser tout ordinateur s'y trouvant pour vérifier les données que celui-ci contient ou auxquelles il donne accès;

(*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.

b) reproduire ou faire reproduire des données sous forme d'imprimé ou toute autre forme intelligible;

c) saisir tout imprimé ou sortie de données pour examen ou reproduction;

d) utiliser ou faire utiliser le matériel s'y trouvant pour reproduire des données.

. . .

487.01 (1) Un juge de la cour provinciale, un juge de la cour supérieure de juridiction criminelle ou un juge au sens de l'article 552 peut décerner un mandat par écrit autorisant un agent de la paix, sous réserve du présent article, à utiliser un dispositif ou une technique ou une méthode d'enquête, ou à accomplir tout acte qui y est mentionné, qui constituerait sans cette autorisation une fouille, une perquisition ou une saisie abusive à l'égard d'une personne ou d'un bien :

a) si le juge est convaincu, à la suite d'une dénonciation par écrit faite sous serment, qu'il existe des motifs raisonnables de croire qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements relatifs à l'infraction seront obtenus grâce à une telle utilisation ou à l'accomplissement d'un tel acte;

b) s'il est convaincu que la délivrance du mandat servirait au mieux l'administration de la justice;

c) s'il n'y a aucune disposition dans la présente loi ou toute autre loi fédérale qui prévoie un mandat, une autorisation ou une ordonnance permettant une telle utilisation ou l'accomplissement d'un tel acte.

. . .

(3) Le mandat doit énoncer les modalités que le juge estime opportunes pour que la fouille, la perquisition ou la saisie soit raisonnable dans les circonstances.

. . .

(5.1) Le mandat qui autorise l'agent de la paix à perquisitionner secrètement doit exiger, dans le cadre des modalités visées au paragraphe (3), qu'un avis de la perquisition soit donné dans le délai suivant son exécution que le juge estime indiqué dans les circonstances.

. . .

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.

. . .

487.012 (1) Sauf si elle fait l'objet d'une enquête relative à l'infraction visée à l'alinéa (3)*a*), un juge de paix ou un juge peut ordonner à une personne :

a) de communiquer des documents — originaux ou copies certifiées conformes par affidavit — ou des données;

b) de préparer un document à partir de documents ou données existants et de le communiquer.

(2) L'ordonnance précise le moment, le lieu et la forme de la communication ainsi que la personne à qui elle est faite — agent de la paix ou fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale.

(3) Le juge de paix ou le juge ne rend l'ordonnance que s'il est convaincu, à la suite d'une dénonciation par écrit faite sous serment et présentée *ex parte*, qu'il existe des motifs raisonnables de croire que les conditions suivantes sont réunies :

a) une infraction à la présente loi ou à toute autre loi fédérale a été ou est présumée avoir été commise;

b) les documents ou données fourniront une preuve touchant la perpétration de l'infraction;

c) les documents ou données sont en la possession de la personne en cause ou à sa disposition.

(4) L'ordonnance peut être assortie des conditions que le juge de paix ou le juge estime indiquées, notamment pour protéger les communications privilégiées entre l'avocat — et, dans la province de Québec, le notaire — et son client.

Pourvoi accueilli, la juge en chef McLachlin *et le juge* Cromwell *sont dissidents.*

Procureurs de l'appelante : 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.

Procureur de l'intimée : Service des poursuites pénales du Canada, Toronto.

Procureur de l'intervenant le procureur général de l'Ontario : Procureur général de l'Ontario, Toronto.

Procureurs de l'intervenante l'Association canadienne des libertés civiles : Torys, Toronto.

Procureur de l'intervenante la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko : Université d'Ottawa, Ottawa.