Tristin Jones *Appellant*

v.

Her Majesty The Queen in Right of Canada and Her Majesty The Queen in Right of Ontario *Respondents*

and

Attorney General of British Columbia, Director of Criminal and Penal Prosecutions, Criminal Lawyers' Association of Ontario, Canadian Civil Liberties Association, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic and British Columbia Civil Liberties Association *Interveners*

Indexed as: R. *v.* Jones

2017 SCC 60

File No.: 37194.

2017: March 23; 2017: December 8.

Present: McLachlin C.J. and Abella, Moldaver, Karakatsanis, Gascon, Côté and Rowe JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO

Constitutional law — Charter of Rights — Enforcement — Standing — Search and seizure — Evidence — Admissibility — Text messages — Accused seeking to exclude at trial text message records obtained by production order from telecommunications service provider — Whether accused has reasonable expectation of privacy in text messages stored by service provider and therefore standing under s. 8 of Canadian Charter of Rights and Freedoms to challenge production order — Whether accused permitted to rely on Crown theory for purposes of establishing subjective expectation of privacy.

Criminal law — Evidence — Production orders — Invasion of privacy — Interception of communications —

Tristin Jones *Appelant*

c.

Sa Majesté la Reine du chef du Canada et Sa Majesté la Reine du chef de l'Ontario *Intimées*

et

Procureur général de la Colombie-Britannique, directeur des poursuites criminelles et pénales, Criminal Lawyers' Association of Ontario, Association canadienne des libertés civiles, Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko et British Columbia Civil Liberties Association *Intervenants*

Répertorié : R. *c.* Jones

2017 CSC 60

N° du greffe : 37194.

2017 : 23 mars; 2017 : 8 décembre.

Présents : La juge en chef McLachlin et les juges Abella, Moldaver, Karakatsanis, Gascon, Côté et Rowe.

EN APPEL DE LA COUR D'APPEL DE L'ONTARIO

Droit constitutionnel — Charte des droits — Application — Qualité pour agir — Fouilles, perquisitions et saisies — Preuve — Admissibilité — Messages textes — Demande de l'accusé en vue de faire écarter au procès des relevés contenant des messages textes obtenus d'un fournisseur de services de télécommunications au moyen d'une ordonnance de communication — L'accusé a-t-il une attente raisonnable au respect de sa vie privée à l'égard des copies des messages textes conservées par le fournisseur de services et, en conséquence, qualité pour contester l'ordonnance de communication en vertu de l'art. 8 de la Charte canadienne des droits et libertés? — L'accusé est-il autorisé à s'appuyer sur la thèse de la Couronne afin d'établir son attente subjective au respect de sa vie privée?

Droit criminel — Preuve — Ordonnances de communication — Atteinte à la vie privée — Interception de

Police obtaining order under s. 487.012 of Criminal Code for production of text messages stored on service provider's infrastructure — Whether production order provides lawful authority for seizing stored text messages or whether wiretap authorization under Part VI of Criminal Code required for seizure to comply with s. 8 of Canadian Charter of Rights and Freedoms — Criminal Code, R.S.C. 1985, c. C-46, ss. 183 "intercept", 487.012.

J was convicted of several firearms and drug trafficking offences. His convictions rest on records of text messages seized from a Telus account associated with his co-accused that were obtained under a production order pursuant to s. 487.012 of the *Criminal Code* (now s. 487.014). Prior to trial, J sought to exclude the text messages on the basis that obtaining them by means of a production order contravened his s. 8 *Charter* right. The trial judge found that J lacked standing to challenge the production order under s. 8 and he was therefore convicted. J's appeal against conviction was dismissed.

Held (Abella J. dissenting): The appeal should be dismissed and the production order upheld.

Per McLachlin C.J. and Moldaver, Karakatsanis, Gascon and Côté JJ.: J had a reasonable expectation of privacy in the text messages stored by Telus and therefore standing under s. 8 of the *Charter* to challenge the production order. Whether a claimant has a reasonable expectation of privacy must be answered with regard to the totality of the circumstances of a particular case. Claimants must establish that they had a direct interest in the subject matter of the search, that they had a subjective expectation of privacy in that subject matter and that their subjective expectation of privacy was objectively reasonable.

In this case, the subject matter of the search is the electronic conversation between J and his co-accused. J should have been permitted to rely on the Crown's theory that he authored those text messages for the purposes of establishing his direct interest in their subject matter and his subjective expectation of privacy in the messages. An accused mounting a s. 8 *Charter* claim may

communications — Obtention par les policiers d'une ordonnance prévue à l'art. 487.012 du Code criminel en vue de se faire communiquer des messages textes conservés dans l'infrastructure du fournisseur de services — Une ordonnance de communication permet-elle de saisir légalement de tels messages ou est-il nécessaire d'obtenir une autorisation de mise sous écoute électronique en vertu de la partie VI du Code criminel pour que la saisie respecte l'art. 8 de la Charte canadienne des droits et libertés? — Code criminel, L.R.C. 1985, c. C-46, art. 183 « intercepter », 487.012.

J a été déclaré coupable de plusieurs infractions liées au trafic d'armes à feu et de drogues. Ces déclarations de culpabilité reposent sur des relevés contenant des messages textes qui ont été saisis d'un compte Telus associé à son coaccusé en application d'une ordonnance de communication obtenue en vertu de l'art. 487.012 du *Code criminel* (maintenant l'art. 487.014). Avant le procès, J a tenté de faire écarter les messages textes au motif que leur obtention au moyen d'une ordonnance de communication avait contrevenu aux droits que lui garantit l'art. 8 de la *Charte*. La juge du procès a conclu que J n'avait pas qualité pour contester l'ordonnance de communication sur le fondement de l'art. 8 et ce dernier a par conséquent été déclaré coupable. L'appel interjeté par J à l'encontre de sa déclaration de culpabilité a été rejeté.

Arrêt (la juge Abella est dissidente) : Le pourvoi est rejeté et l'ordonnance de communication est confirmée.

La juge en chef McLachlin et les juges Moldaver, Karakatsanis, Gascon et Côté : J avait une attente raisonnable au respect de sa vie privée relativement aux messages textes conservés par Telus et, en conséquence, il avait qualité pour contester la validité de l'ordonnance de communication en vertu de l'art. 8 de la *Charte*. Pour répondre à la question de savoir si l'auteur d'une telle demande a une attente raisonnable au respect de sa vie privée, il faut tenir compte de l'ensemble des circonstances propres à l'affaire en cause. L'auteur de la demande doit prouver qu'il avait un droit direct à l'égard de l'objet de la fouille, qu'il avait une attente subjective en matière de respect de sa vie privée à l'égard de l'objet de cette fouille et que son attente subjective en matière de respect de la vie privée était objectivement raisonnable.

En l'espèce, l'objet de la fouille est la conversation électronique entre J et son coaccusé. J aurait dû être autorisé à s'appuyer sur la thèse de la Couronne selon laquelle il était l'auteur de ces messages textes afin d'établir son droit direct à l'égard de l'objet de la fouille et son attente subjective au respect de sa vie privée à l'égard des messages. Un accusé qui invoque l'art. 8 de la *Charte* peut

ask the court to assume as true any fact that the Crown has alleged or will allege in the prosecution against him in lieu of tendering evidence probative of those same facts in the *voir dire*. This coheres with the relatively modest evidentiary foundation required to establish the subjective expectation element in the totality of the circumstances analysis, as well as the principle against self-incrimination.

It follows that J subjectively expected privacy in records of his electronic conversation found in the service provider's infrastructure. Text messages are private communications. This is not in dispute in this case. Moreover, as the application judge found, J and his co-accused used third-party names so as to avoid detection or association with the text messages. This suggests that they intended their communications to remain private.

Finally, it is objectively reasonable for the sender of a text message to expect a service provider to keep information private where its receipt and retention of such information is incidental to its role of delivering private communications to the intended recipient. That is intuitive. One would not reasonably expect the service provider to share the text messages with an unintended recipient, or post them publicly for the world to see. In this case, it was therefore reasonable for J to expect that the text messages that he sent would not be shared by Telus with any parties other than the intended recipient, notwithstanding that he relinquished direct control over those messages. Neither the absence of a contractual policy, nor the fact that the production order targeted a phone registered to a third party, deprives J of that protection.

On the totality of the circumstances, therefore, J had a reasonable expectation of privacy in the text messages and standing to challenge the validity of the production order. However, J's s. 8 *Charter* right was not breached because records of text messages stored on a service provider's infrastructure were lawfully seized by means of a production order under s. 487.012 of the *Criminal Code*. Based on its plain meaning and read in context, the term "intercept" in s. 183 of Part VI of the *Criminal Code* does not encompass the production or seizure

demander au tribunal de tenir pour avéré tout fait que la Couronne allègue ou entend alléguer dans les poursuites intentées contre lui, au lieu de devoir présenter des éléments de preuve établissant ces mêmes faits lors du voir-dire. Ce résultat s'accorde avec le fait qu'une preuve relativement minime est requise pour démontrer l'existence de l'attente subjective dans le cadre de l'analyse de l'ensemble des circonstances, ainsi qu'avec le principe protégeant contre l'auto-incrimination.

Il s'ensuit que J s'attendait subjectivement à ce que l'on respecte son droit à la vie privée relativement aux copies de sa conversation électronique se trouvant dans l'infrastructure du fournisseur de services. Les messages textes constituent des communications privées. Cela n'est pas contesté en l'espèce. De plus, comme a conclu la juge saisie de la demande, J et son coaccusé se sont servis de noms de tiers pour éviter d'être repérés ou d'être associés aux messages textes. Cela tend à indiquer qu'ils entendaient que leurs communications demeurent privées.

Enfin, il est objectivement raisonnable de la part de l'expéditeur de messages textes de s'attendre à ce qu'un fournisseur de services protège le caractère privé de l'information qui lui est confiée, dans les cas où la réception et la conservation de cette information constituent un aspect accessoire de son rôle consistant à acheminer des communications privées au destinataire visé. Cette conclusion a un caractère intuitif. Il ne serait pas raisonnable de s'attendre à ce qu'un fournisseur de services communique les messages textes à un destinataire non visé ou qu'il les mette à la disposition du monde entier. Dans le cas qui nous occupe, il était donc raisonnable de la part de J de s'attendre à ce que Telus ne communiquerait à personne d'autre qu'au destinataire visé les messages textes qu'il envoyait, malgré le fait qu'il ait renoncé à exercer un contrôle direct sur ces messages. Ni l'absence de politique de confidentialité de nature contractuelle ni le fait que l'ordonnance de communication visait un téléphone enregistré au nom d'un tiers ne privent J de cette protection.

Par conséquent, au regard de l'ensemble des circonstances, J avait une attente raisonnable au respect de sa vie privée relativement aux messages textes en cause, et il avait qualité pour contester la validité de l'ordonnance de communication. Toutefois, les droits garantis à J par l'art. 8 de la *Charte* n'ont pas été violés, étant donné que les relevés contenant les messages textes conservés dans l'infrastructure du fournisseur de services ont été saisis légalement au moyen de l'ordonnance de communication prévue à l'art. 487.012 du *Code criminel*. Selon son sens

of historical text messages stored by a service provider. Historical text messages denote messages that have been sent and received, not those still in the transmission process. In this case, there is no question that Telus initially intercepted the communications between J and his co-accused, presumably pursuant to an exception for service delivery purposes under s. 184(2) of the *Criminal Code*. However, in light of the statutory scheme's distinction between interception, use and retention, and disclosure, it is clear that Telus' subsequent storing and provision of the communications to the law enforcement did not constitute additional interceptions. Rather, Telus retained the intercepted communications under s. 184(3) and then disclosed them to the police as contemplated by s. 193(2) of the *Criminal Code*.

In this case, a Part VI wiretap authorization was unnecessary because the police did not seek an order authorizing the prospective production of future text messages. Nor is there any evidence that the production order resulted in the production of text messages that were still in the transmission process. Therefore, the search and seizure of J's text messages were properly authorized by the production order provision in s. 487.012 of the *Criminal Code*, and did not breach J's s. 8 *Charter* right.

Per Rowe J.: There is agreement with the majority that, as a matter of statutory interpretation, a production order pursuant to s. 487.012 of the *Criminal Code* (now s. 487.014) authorizes the police to request the disclosure of text messages from a service provider once those messages have been sent and received. Conversely, a Part VI *Criminal Code* authorization is required to intercept those messages as they are being transmitted. Given that the records of text messages are stored by the service provider in this case the moment they are sent, however, it makes little difference whether the police "intercept" them or simply obtain them through a production order immediately after they are sent. It appears that the police can in effect sidestep the requirements of Part VI by obtaining a production order immediately after the messages are sent. No settled view is expressed as to whether this anomaly reflects a failure of s. 487.014 to meet the

courant et à la lumière de son contexte, le mot « intercepter » à l'art. 183 de la partie VI du *Code criminel* ne couvre pas la communication ou la saisie de messages textes existants conservés par un fournisseur de services. Les messages textes existants s'entendent des messages qui ont été expédiés et reçus, non pas de ceux qui sont encore en cours de transmission. Dans le cas qui nous occupe, il ne fait aucun doute que les communications échangées entre J et son coaccusé ont initialement été interceptées par Telus, vraisemblablement en vertu d'une des exceptions prévues au par. 184(2) du *Code criminel* pour les besoins de la fourniture des services. Toutefois, compte tenu de la distinction que le régime législatif établit entre l'interception, l'utilisation et la conservation d'une part, ainsi que la divulgation d'autre part, il est évident que la conservation des télécommunications par Telus et leur divulgation ultérieure par cette dernière aux policiers n'ont pas constitué des interceptions additionnelles. Telus a plutôt conservé les communications interceptées en vertu du par. 184(3), puis les a ensuite divulguées aux policiers comme le prévoit le par. 193(2) du *Code criminel*.

En l'espèce, il n'était pas nécessaire d'obtenir l'autorisation d'écoute électronique prévue à la partie VI, étant donné que les policiers ne sollicitaient pas une ordonnance les autorisant à obtenir la production prospective de messages textes futurs. Rien ne prouve non plus que l'ordonnance de communication a entraîné la communication de messages textes qui se trouvaient encore dans le processus de transmission. Par conséquent, la fouille et la saisie des messages textes de J ont été régulièrement autorisées en vertu des dispositions relatives aux ordonnances de communication figurant à l'art. 487.012 du *Code criminel*, et ces mesures n'ont pas porté atteinte aux droits garantis à J par l'art. 8 de la *Charte*.

Le juge Rowe : Il y a accord avec la conclusion des juges majoritaires selon laquelle, suivant les règles d'interprétation des lois, l'ordonnance de communication prévue à l'art. 487.012 du *Code criminel* (maintenant l'art. 487.014) autorise les policiers à demander à un fournisseur de services de divulguer des messages textes après que ceux-ci ont été envoyés et reçus. En revanche, une autorisation fondée sur la partie VI du *Code criminel* est requise pour intercepter ces messages pendant leur transmission. Cependant, comme le fournisseur de services concerné en l'espèce conserve des copies des messages textes dès qu'ils sont envoyés, il importe peu que les policiers les « interceptent » ou les obtiennent tout simplement au moyen d'une ordonnance de communication immédiatement après leur envoi. Il semble que les policiers peuvent effectivement éluder les exigences de la partie VI en obtenant une ordonnance de

requirements imposed by s. 8 of the *Charter* because this issue was not raised in argument.

Per Abella J. (dissenting): There is agreement with the majority that J had a reasonable expectation of privacy in his sent text messages and, as a result, had standing under s. 8 of the *Charter* to challenge the production order. But since the messages were obtained pursuant to a production order rather than a Part VI *Criminal Code* authorization, the search and seizure of those messages was not authorized by law and was therefore unreasonable.

The police obtained several production orders pursuant to s. 487.012 of the *Criminal Code* directed at the service providers Bell, Rogers and Telus. Only Telus stored the content of incoming and outgoing text messages for a period of time after the messages were sent and received. No text messages were obtained from accounts held with the other service providers. Telus' unique storage practices, rather than the underlying principles in Part VI, led to the production of copies of historical text messages from the targeted Telus account, and the loss of J's privacy protections available under Part VI. By prioritizing a temporal distinction to determine the level of privacy protection for text messages, Telus customers are left with less protection than those using other service providers who do not store copies of text messages simply because Telus stores copies of text messages that pass through its infrastructure. This means that the privacy rights of those who text depend on which service provider they use rather than on the fact that they are texting as a means of privately communicating.

The term "intercept" in s. 183 of the *Criminal Code* should be interpreted in the context of the broader Part VI scheme and the purpose it is meant to serve, namely, to prevent the state from acquiring private communications without lawful authorization and to protect the privacy interests inherent in the content of private communications. The Part VI protections should be available for historical as well as for prospective interception. The timing of the state's request for information should not distort the

communication immédiatement après l'envoi des messages. Aucune opinion définitive n'est exprimée quant à la question de savoir si ces anomalies indiquent que l'art. 487.014 ne respecte pas les exigences de l'art. 8 de la *Charte*, étant donné que cette question n'a pas été soulevée lors des débats.

La juge Abella (dissidente) : Il y a accord avec la conclusion des juges majoritaires suivant laquelle J possédait une attente raisonnable au respect de sa vie privée à l'égard des messages textes qu'il a envoyés et que, par conséquent, il avait qualité pour contester l'ordonnance de communication en vertu de l'art. 8 de la *Charte*. Mais puisque les messages ont été obtenus aux termes d'une ordonnance de communication plutôt que d'une autorisation sous le régime de la partie VI du *Code criminel*, la fouille et la saisie de ces messages n'étaient pas autorisées par la loi et étaient donc abusives.

Les policiers ont obtenu, en vertu de l'art. 487.012 du *Code criminel*, plusieurs ordonnances de communication visant les fournisseurs de services Bell, Rogers et Telus. Seule la société Telus conserve pendant une certaine période le contenu des messages textes envoyés et reçus par ses abonnés. Aucun message texte n'a été obtenu à partir de comptes existants auprès d'autres fournisseurs de services. Ce sont les pratiques de stockage uniques à Telus, plutôt que les principes qui sous-tendent la partie VI, qui ont mené à la communication des copies de messages textes existants du compte Telus visé, et à la perte par J des mesures de protection de la vie privée prévues par la partie VI. Si on privilégie une distinction d'ordre temporel pour déterminer le degré de protection de la vie privée applicable à l'égard des messages textes, les clients de Telus se trouvent alors à bénéficier d'une protection inférieure à celle dont jouissent les clients faisant appel à d'autres fournisseurs de services qui ne conservent pas de copies des messages textes, et ce, tout simplement parce que Telus conserve des copies des messages textes qui passent par son infrastructure. Cela signifie que le droit des auteurs de messages textes au respect de leur vie privée dépend de l'identité de leur fournisseur de services, plutôt que du fait qu'ils utilisent les messages textes comme moyen de communiquer privément.

Le mot « intercepter » à l'art. 183 du *Code criminel* devrait être interprété dans le contexte général du régime de la partie VI et de l'objet que celui-ci est censé viser, c'est-à-dire prévenir l'acquisition par l'État de communications privées sans autorisation valable et protéger le droit intrinsèque au respect de la vie privée à l'égard du contenu de communications privées. Les protections qu'offre la partie VI devraient s'appliquer à l'interception des messages textes existants ainsi que des messages

communicative dimension of a text message exchange. Interpreting "intercept[ion]" of a private communication should focus on the content, not on the timing, of what the investigative technique seeks to access, or on the vagaries of the service provider's technological practices.

When the police obtain copies of text messages from a service provider, they are acquiring a complete record of all electronic conversations that took place during a given period. The informational content acquired by the state is a complete record of all private communications in the given period. A singular focus on the *historical* dimension of the record should not detract from the content and character of this record. It is a record of a conversation that took place between individuals, albeit in an electronic format, that has been assigned a specific timestamp. This record may capture electronic conversations between several people innocently participating in an electronic conversation with the targeted recipient, as well as electronic conversations involving multiple participants engaged in a group text.

Since no Part VI authorization was obtained, the acquisition of copies of J's historical text messages through the production order was invalid and breached J's rights under s. 8 of the *Charter*.

The messages should be excluded under s. 24(2) of the *Charter*. The evolution of shifting technology has resulted in a correspondingly evolving jurisprudence which tries to keep pace with the impact of technology on constitutional rights. Where no case directly on point has been decided, the police have two choices: to use the jurisprudential gap as a rationale for being more intrusive, or to exercise greater caution before interfering with legislatively endorsed privacy rights. The better judicial approach is one that encourages conduct on the part of the police that errs on the side of being protective of the rights of the public, rather than one that endorses *Charter* breaches in deference to the mechanics of new technologies.

textes futurs. Le moment où l'État présente sa demande d'information ne devrait pas dénaturer la dimension communicationnelle d'un échange de messages textes. L'interprétation du terme « intercept[ion] » d'une communication privée doit s'attacher à la substance des éléments auxquels la technique d'enquête vise à obtenir accès, et non au moment où cet accès est demandé, ou encore au hasard des pratiques technologiques des fournisseurs de services.

Lorsque les policiers obtiennent d'un fournisseur de services des copies de messages textes, ils prennent connaissance d'un relevé complet de l'ensemble des conversations électroniques qui ont eu lieu au cours de la période donnée. Le contenu informationnel dont prend connaissance l'État est un relevé complet de l'ensemble des communications privées survenues au cours d'une période donnée. L'insistance particulière sur le fait que le relevé porte sur des messages textes *existants* ne devrait pas faire oublier le contenu et la nature de ce relevé. Il s'agit d'un relevé reproduisant le texte d'une conversation qui a eu lieu entre des personnes, même si elle a pris une forme électronique, et à laquelle on a assigné un repère temporel précis. Ce relevé pourrait comprendre des conversations électroniques entre plusieurs personnes qui participent innocemment à une conversation électronique avec le destinataire visé, ainsi que des conversations électroniques entre de multiples participants à un échange de messages textes au sein d'un groupe.

Comme aucune autorisation fondée sur la partie VI n'a été obtenue, la prise de connaissance des copies des messages textes existants de J obtenues au moyen d'une ordonnance de communication était invalide et violait les droits garantis à ce dernier par l'art. 8 de la *Charte*.

Les messages devraient être écartés en vertu du par. 24(2) de la *Charte*. L'évolution rapide de la technologie entraîne une évolution correspondante de la jurisprudence, laquelle s'efforce de suivre le rythme de l'incidence de la technologie sur les droits garantis par la Constitution. Dans les cas où aucune décision portant exactement sur une situation litigieuse n'a encore été rendue, les policiers ont alors le choix entre deux possibilités : utiliser la lacune dans la jurisprudence pour justifier une conduite plus envahissante, ou exercer davantage de précaution avant de porter atteinte à des droits protégeant la vie privée garantis par la loi. La meilleure approche à adopter par les tribunaux consiste à inciter les policiers à pécher par excès de prudence afin de protéger les droits du public, plutôt qu'à cautionner des violations de la *Charte* par déférence pour la mécanique des nouvelles technologies.

The impact of the *Charter*-infringing conduct on J's *Charter*-protected privacy interests under s. 8 of the *Charter* was significant. Whether they take the form of a historical record or occur in real-time, electronic conversations have the potential to reveal information going to the individual's biographical core, including information which tends to reveal intimate details of the lifestyle or personal choices of an individual. While the police did not technically act in bad faith, their failure to seek Part VI authorization put public confidence in the administration of justice at serious risk. The impact of their conduct on J's considerable, *Charter*-protected privacy interests under s. 8 of the *Charter* was significant, which outweighs the public's interest in seeing a determination of J's case on the merits.

Cases Cited

By Côté J.

Applied: *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; **considered:** *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *R. v. Shayesteh* (1996), 31 O.R. (3d) 161; *R. v. Duarte*, [1990] 1 S.C.R. 30; **referred to:** *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Gauthier*, [1977] 1 S.C.R. 441; *R. v. Jir*, 2010 BCCA 497, 264 C.C.C. (3d) 64; *R. v. Hurry*, 2002 ABQB 420, 165 C.C.C. (3d) 182; *R. v. Henry*, 2005 SCC 76, [2005] 3 S.C.R. 609; *R. v. Nedelcu*, 2012 SCC 59, [2012] 3 S.C.R. 311; *R. v. Hart*, 2014 SCC 52, [2014] 2 S.C.R. 544; *R. v. Jones*, [1994] 2 S.C.R. 229; *R. v. White*, [1999] 2 S.C.R. 417; *R. v. Big M Drug Mart Ltd.*, [1985] 1 S.C.R. 295; *R. v. Golden*, 2001 SCC 83, [2001] 3 S.C.R. 679; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Stillman*, [1997] 1 S.C.R. 607; *R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227; *R. v. Pugliese* (1992), 71 C.C.C. (3d) 295; *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27; *R. v. Belcourt*, 2015 BCCA 126, 322 C.C.C. (3d) 93; *R. v. McQueen* (1975), 25 C.C.C. (2d) 262; *R. v. Giles*, 2007 BCSC 1147; *R. v. Beauchamp*, 2015 ONCA 260, 326 C.C.C. (3d) 280; *R. v. Finlay* (1985), 23 C.C.C. (3d) 48; *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657.

Les répercussions de la conduite attentatoire à la *Charte* sur le droit à la protection de la vie privée garanti à J par l'art. 8 de ce texte ont été importantes. Qu'il s'agisse de messages existants ou d'un échange en temps réel, les conversations électroniques sont susceptibles de révéler des renseignements biographiques sur les gens, notamment des renseignements qui tendent à révéler des détails intimes sur leur mode de vie et leurs choix personnels. Bien que la police n'ait pas, techniquement, agi de mauvaise foi, le défaut d'obtenir une autorisation sous le régime de la partie VI a sérieusement compromis la confiance du public envers l'administration de la justice. Les répercussions de la conduite des policiers sur le droit au respect de la vie privée garanti à J par l'art. 8 de la *Charte* ont été importantes, facteur qui l'emporte sur l'intérêt du public à ce qu'un jugement au fond soit rendu.

Jurisprudence

Citée par la juge Côté

Arrêt appliqué : *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212; **arrêts examinés :** *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3; *R. c. Shayesteh* (1996), 31 O.R. (3d) 161; *R. c. Duarte*, [1990] 1 R.C.S. 30; **arrêts mentionnés :** *R. c. Edwards*, [1996] 1 R.C.S. 128; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Collins*, [1987] 1 R.C.S. 265; *R. c. Wong*, [1990] 3 R.C.S. 36; *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *R. c. Gauthier*, [1977] 1 R.C.S. 441; *R. c. Jir*, 2010 BCCA 497, 264 C.C.C. (3d) 64; *R. c. Hurry*, 2002 ABQB 420, 165 C.C.C. (3d) 182; *R. c. Henry*, 2005 CSC 76, [2005] 3 R.C.S. 609; *R. c. Nedelcu*, 2012 CSC 59, [2012] 3 R.C.S. 311; *R. c. Hart*, 2014 CSC 52, [2014] 2 R.C.S. 544; *R. c. Jones*, [1994] 2 R.C.S. 229; *R. c. White*, [1999] 2 R.C.S. 417; *R. c. Big M Drug Mart Ltd.*, [1985] 1 R.C.S. 295; *R. c. Golden*, 2001 CSC 83, [2001] 3 R.C.S. 679; *R. c. Dyment*, [1988] 2 R.C.S. 417; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Stillman*, [1997] 1 R.C.S. 607; *R. c. Law*, 2002 CSC 10, [2002] 1 R.C.S. 227; *R. c. Pugliese* (1992), 71 C.C.C. (3d) 295; *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211; *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 R.C.S. 27; *R. c. Belcourt*, 2015 BCCA 126, 322 C.C.C. (3d) 93; *R. c. McQueen* (1975), 25 C.C.C. (2d) 262; *R. c. Giles*, 2007 BCSC 1147; *R. c. Beauchamp*, 2015 ONCA 260, 326 C.C.C. (3d) 280; *R. c. Finlay* (1985), 23 C.C.C. (3d) 48; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992; *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657.

By Abella J. (dissenting)

R. v. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608; *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *R. v. Hoelscher*, 2016 ABQB 44; *R. v. Croft*, 2013 ABQB 640, 304 C.C.C. (3d) 279; *R. v. Carty*, 2014 ONSC 212; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Paterson*, 2017 SCC 15, [2017] 1 S.C.R. 202; *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 7, 8, 13, 24(2).

Criminal Code, R.S.C. 1985, c. C-46, ss. 99, 164.2(1)(b)(ii), 164.3(4)(b), 182(2)(e), Part VI, 183 "authorization", "intercept", "private communication", 183 to 196, 184, 184 to 192, 193, 462.34(6)(a)(ii), 462.41(3)(b), 462.42(1)(b), 487, 487.01(1)(c), 487.012 [ad. 2004, c. 3, s. 7], 487.014 [ad. 2014, c. 31, s. 20; formerly s. 487.012], 490.4(3), 490.5(1)(c).

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 3, 5(3), 7.

Authors Cited

Driedger, Elmer A. *Construction of Statutes*, 2nd ed. Toronto: Butterworths, 1983.

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 9th ed. Toronto: LexisNexis, 2015.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, vol. 1. Toronto: Carswell, 1991 (loose-leaf updated 2017, release 7).

Magotiaux, Susan. "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015), 71 *S.C.L.R.* (2d) 501.

Penney, Steven. "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014), 67 *S.C.L.R.* (2d) 505.

Stewart, Hamish. "Normative Foundations for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335.

APPEAL from a judgment of the Ontario Court of Appeal (MacPherson, MacFarland and LaForme JJ.A.), 2016 ONCA 543, 131 O.R. (3d) 604, 361 C.R.R. (2d) 350, 338 C.C.C. (3d) 591, 350 O.A.C. 274, [2016] O.J. No. 3737 (QL), 2016 CarswellOnt 10858 (WL Can.), affirming the accused's convictions for firearms and drug trafficking offences and

Citée par la juge Abella (dissidente)

R. c. Marakah, 2017 CSC 59, [2017] 2 R.C.S. 608; *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3; *R. c. Hoelscher*, 2016 ABQB 44; *R. c. Croft*, 2013 ABQB 640, 304 C.C.C. (3d) 279; *R. c. Carty*, 2014 ONSC 212; *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353; *R. c. Paterson*, 2017 CSC 15, [2017] 1 R.C.S. 202; *R. c. Côté*, 2011 CSC 46, [2011] 3 R.C.S. 215.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 7, 8, 13, 24(2).

Code criminel, L.R.C. 1985, c. C-46, art. 99, 164.2(1)b)(ii), 164.3(4)b), 182(2)e), partie VI, 183 « autorisation », « communication privée », « intercepter », 183 à 196, 184, 184 à 192, 193, 462.34(6)a)(ii), 462.41(3), 462.42(1), 487, 487.01(1)c), 487.012 [aj. 2004, c. 3, art. 7], 487.014 [aj. 2014, c. 31, art. 20; auparavant art. 487.012], 490.4(3), 490.5(1)c).

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5, art. 3, 5(3), 7.

Doctrine et autres documents cités

Driedger, Elmer A. *Construction of Statutes*, 2nd ed., Toronto, Butterworths, 1983.

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 9th ed., Toronto, LexisNexis, 2015.

Hutchison, Scott C., et al. *Search and Seizure Law in Canada*, vol. 1, Toronto, Carswell, 1991 (loose-leaf updated 2017, release 7).

Magotiaux, Susan. « Out of Sync : Section 8 and Technological Advancement in Supreme Court Jurisprudence » (2015), 71 *S.C.L.R.* (2d) 501.

Penney, Steven. « The Digitization of Section 8 of the Charter : Reform or Revolution? » (2014), 67 *S.C.L.R.* (2d) 505.

Stewart, Hamish. « Normative Foundations for Reasonable Expectations of Privacy » (2011), 54 *S.C.L.R.* (2d) 335.

POURVOI contre un arrêt de la Cour d'appel de l'Ontario (les juges MacPherson, MacFarland et LaForme), 2016 ONCA 543, 131 O.R. (3d) 604, 361 C.R.R. (2d) 350, 338 C.C.C. (3d) 591, 350 O.A.C. 274, [2016] O.J. No. 3737 (QL), 2016 CarswellOnt 10858 (WL Can.), qui a confirmé les déclarations de culpabilité prononcées contre l'accusé pour des

the pre-trial application ruling. Appeal dismissed, Abella J. dissenting.

Patrick McCann, *Peter Mantas* and *Ewan Lyttle*, for the appellant.

Nicholas E. Devlin and *Jennifer Conroy*, for the respondent Her Majesty The Queen in Right of Canada.

Randy Schwartz and *Andrew Hotke*, for the respondent Her Majesty The Queen in Right of Ontario.

Written submissions only by *Daniel M. Scanlan*, for the intervener the Attorney General of British Columbia.

Ann Ellefsen-Tremblay and *Daniel Royer*, for the intervener the Director of Criminal and Penal Prosecutions.

Susan M. Chapman, *Naomi Greckol-Herlich* and *Bianca Bell*, for the intervener the Criminal Lawyers' Association of Ontario.

Christine Lonsdale and *Charlotte-Anne Malischewski*, for the intervener the Canadian Civil Liberties Association.

Jill R. Presser and *David A. Fewer*, for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

Gerald Chan, for the intervener the British Columbia Civil Liberties Association.

The judgment of McLachlin C.J. and Moldaver, Karakatsanis, Gascon and Côté JJ. was delivered by

CÔTÉ J. —

I. Overview

[1] The appellant, Mr. Jones, was convicted of several firearms and drug trafficking offences. His

infractions liées au trafic d'armes à feu et de drogues, ainsi que sur la requête présentée avant le procès. Pourvoi rejeté, la juge Abella est dissidente.

Patrick McCann, *Peter Mantas* et *Ewan Lyttle*, pour l'appelant.

Nicholas E. Devlin et *Jennifer Conroy*, pour l'intimée Sa Majesté la Reine du chef du Canada.

Randy Schwartz et *Andrew Hotke*, pour l'intimée Sa Majesté la Reine du chef de l'Ontario.

Argumentation écrite seulement par *Daniel M. Scanlan*, pour l'intervenant le procureur général de la Colombie-Britannique.

Ann Ellefsen-Tremblay et *Daniel Royer*, pour l'intervenant le directeur des poursuites criminelles et pénales.

Susan M. Chapman, *Naomi Greckol-Herlich* et *Bianca Bell*, pour l'intervenante Criminal Lawyers' Association of Ontario.

Christine Lonsdale et *Charlotte-Anne Malischewski*, pour l'intervenante l'Association canadienne des libertés civiles.

Jill R. Presser et *David A. Fewer*, pour l'intervenante la Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko.

Gerald Chan, pour l'intervenante British Columbia Civil Liberties Association.

Version française du jugement de la juge en chef McLachlin et des juges Moldaver, Karakatsanis, Gascon et Côté rendu par

LA JUGE CÔTÉ —

I. Introduction

[1] L'appelant, M. Jones, a été déclaré coupable de plusieurs infractions liées au trafic d'armes à

convictions rest on records of text messages seized from a Telus account associated with his co-accused pursuant to a production order obtained under s. 487.012 (now s. 487.014) of the *Criminal Code*, R.S.C. 1985, c. C-46 ("Production Order"). As in the courts below, the appellant challenges the Production Order under s. 8 of the *Canadian Charter of Rights and Freedoms*. He argues that law enforcement must obtain a "wiretap" authorization under Part VI of the *Code* to seize records of historical text messages from a service provider in order for the seizure to comply with s. 8 of the *Charter*.

[2] His appeal arises out of an Ottawa Police Service investigation into firearms trafficking in the Ottawa, Ontario area. Based on evidence gathered in that investigation, the police obtained the Production Order directing Telus to disclose stored records of any incoming or outgoing text messages on a particular Telus subscriber account associated with the appellant's co-accused, Mr. Waldron. The targeted account was registered in the name of "Kurt Gilles". There is no evidence as to whether Kurt Gilles exists or whether Mr. Waldron merely used that name as an alias for the purposes of his cellphone subscription.

[3] Telus complied with the Production Order and provided the requested records to the police. The records revealed a text message exchange ("Text Messages") concerning the potential transfer of a firearm. The exchange occurred between the Gilles phone and a phone used by the appellant, but registered in the name of his spouse.

[4] Relying in part on the Text Messages, the investigators obtained a *Criminal Code* Part VI authorization ("First Authorization") for a number of phones associated with the suspects. Communications intercepted under it were then used to obtain an additional

feu et de drogues. Ces déclarations de culpabilité reposent sur des relevés contenant des messages textes qui ont été saisis d'un compte Telus associé à son coaccusé, en application d'une ordonnance de communication obtenue en vertu de l'art. 487.012 (maintenant l'art. 487.014) du *Code criminel*, L.R.C. 1985, c. C-46 (« Ordonnance de communication »). Comme il l'a fait devant les juridictions inférieures, l'appelant conteste cette ordonnance en invoquant l'art. 8 de la *Charte canadienne des droits et libertés*. Il soutient que les forces de l'ordre doivent obtenir une autorisation de « mise sur écoute électronique » en vertu de la partie VI du *Code* pour que la saisie auprès d'un fournisseur de services de relevés contenant des messages textes existants respecte l'art. 8 de la *Charte*.

[2] Le présent pourvoi fait suite à une enquête menée par le Service de police d'Ottawa concernant le trafic d'armes à feu dans la région d'Ottawa, en Ontario. Sur la foi d'éléments de preuve recueillis au cours de cette enquête, les policiers ont obtenu l'Ordonnance de communication, laquelle enjoignait à Telus de communiquer des relevés contenant tous les messages textes entrants et sortants d'un compte d'abonné Telus particulier associé à M. Waldron, le coaccusé de l'appelant. Le compte visé était enregistré au nom de « Kurt Gilles ». Il n'y a aucun élément de preuve indiquant si ce Kurt Gilles existe ou non, ou si M. Waldron utilisait simplement ce nom comme pseudonyme pour son compte de téléphonie cellulaire.

[3] Telus s'est conformée à l'Ordonnance de communication et a remis aux policiers les relevés réclamés. Ces relevés ont révélé l'existence d'un échange de messages textes (« Messages textes ») concernant la possible cession d'une arme à feu. Les Messages textes ont été échangés entre le téléphone de M. Gilles et un téléphone utilisé par l'appelant, mais enregistré au nom de sa conjointe.

[4] Se fondant en partie sur les Messages textes, les enquêteurs ont obtenu une autorisation visée à la partie VI du *Code criminel* (« Première autorisation ») à l'égard d'un certain nombre de téléphones associés aux suspects. Les communications

Part VI authorization ("Second Authorization"). On the basis of those subsequent interceptions, search warrants were granted and executed. The fruits of those searches led to the appellant's prosecution for marijuana trafficking and proceeds of crime charges. The firearm trafficking charges against him, on the other hand, were brought largely on the basis of the Text Messages obtained under the Production Order.

[5] Prior to the commencement of the trial, the appellant sought to exclude the Text Messages on the basis that obtaining them by means of a Production Order contravened his s. 8 *Charter* right. Additionally, he challenged the First and Second Authorizations, resulting search warrants and the admissibility of the evidence obtained on the basis of those authorizations insofar as they derived from the Production Order. The latter authorizations and search warrants are not directly at issue on this appeal. Only the Production Order — as lawful authorization — and the Text Messages — as evidence derived therefrom — are in question.

[6] In his s. 8 *Charter* application, the appellant led no evidence demonstrating that he authored and sent the Text Messages. Instead, he argued that he was entitled to rely on the Crown's theory that he was the author of the Text Messages. Applying this Court's decision in *R. v. Edwards*, [1996] 1 S.C.R. 128, the trial judge found that the appellant lacked standing to challenge the Production Order under s. 8 of the *Charter*. The trial judge also dismissed an application to re-open her original s. 8 ruling following the release of this Court's decision in *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3, during Mr. Jones' trial. In doing so, she reasoned that *TELUS* did not address the validity of a production order for obtaining records of historical text messages. The appellant was subsequently

interceptées en application de cette autorisation ont ensuite été utilisées pour obtenir une autre autorisation visée à la partie VI (« Seconde autorisation »). Sur la base de ces interceptions ultérieures, des mandats de perquisition ont été délivrés et exécutés. Les fruits de ces perquisitions ont résulté en des poursuites contre l'appelant pour trafic de marihuana et pour des infractions liées aux produits de la criminalité. Toutefois, les accusations de trafic d'armes à feu portées contre lui reposaient dans une large mesure sur les Messages textes obtenus en vertu de l'Ordonnance de communication.

[5] Avant le début du procès, l'appelant a tenté de faire exclure les Messages textes, au motif que leur obtention au moyen de l'Ordonnance de communication avait contrevenu aux droits qui lui sont garantis par l'art. 8 de la *Charte*. Il a en outre contesté la Première et la Seconde autorisation, les mandats de perquisition délivrés par suite de ces autorisations et l'admissibilité des éléments de preuve recueillis au moyen de ces autorisations, dans la mesure où ces éléments de preuve découlaient de l'Ordonnance de communication. Ces autorisations et mandats de perquisition ne sont pas directement en litige dans le présent pourvoi. Seuls l'Ordonnance de communication — en tant qu'autorisation légitime — ainsi que les Messages textes — en tant qu'éléments de preuve découlant de cette ordonnance —, sont contestés.

[6] Dans sa demande fondée sur l'art. 8 de la *Charte*, l'appelant n'a présenté aucun élément de preuve démontrant qu'il était l'auteur et l'expéditeur des Messages textes. Il a plutôt plaidé qu'il avait le droit de s'appuyer sur la thèse de la Couronne suivant laquelle il était l'auteur des messages en question. Appliquant l'arrêt de notre Cour *R. c. Edwards*, [1996] 1 R.C.S. 128, la juge du procès a conclu que l'appelant n'avait pas qualité pour contester l'Ordonnance de communication sur le fondement de l'art. 8. La juge a également rejeté une demande sollicitant le réexamen de sa décision initiale au sujet de l'art. 8 par suite du prononcé par notre Cour, pendant que se déroulait le procès de M. Jones, de son jugement dans l'affaire *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3.

convicted of several firearms trafficking and drug trafficking offences.

La juge de première instance a justifié le rejet de la demande en expliquant que l'affaire *TELUS* ne portait pas sur la validité d'une ordonnance de communication visant à obtenir des relevés contenant des messages textes existants. L'appelant a subséquemment été reconnu coupable de plusieurs infractions de trafic d'armes à feu et de trafic de drogues.

[7] On appeal, the majority of the Court of Appeal upheld the trial judge's decision regarding the s. 8 standing issue (2016 ONCA 543, 131 O.R. (3d) 604). That was dispositive of the appeal. The majority nevertheless went on to assess the lawfulness of the search at the second stage of the s. 8 inquiry and upheld the use of a production order to obtain records of historical text messages. In separate reasons, LaForme J.A. did not opine on the standing issue, but concurred with the majority's holding regarding the lawfulness of the search. The Court of Appeal was therefore united in its disposition of dismissing the appeal.

[7] En appel, la Cour d'appel a confirmé à la majorité la décision de la juge du procès concernant la qualité pour agir en vertu de l'art. 8 (2016 ONCA 543, 131 O.R. (3d) 604). Cette conclusion était déterminante quant à l'issue de l'appel, mais les juges majoritaires ont néanmoins poursuivi leur examen, se prononçant sur la légalité de la perquisition à la seconde étape de l'analyse fondée sur l'art. 8 et confirmant la validité du recours à une ordonnance de communication pour obtenir des relevés contenant des messages textes existants. Dans des motifs distincts, le juge LaForme n'a pas exprimé d'opinion sur la question de la qualité pour agir, mais il a souscrit à la décision de la majorité sur la légalité de la fouille. La décision de la Cour d'appel rejetant l'appel était par conséquent unanime.

[8] The appeal to this Court raises three questions. First, at his s. 8 *Charter* application, was the appellant entitled to rely on the Crown's theory that he authored the Text Messages in order to establish his subjective expectation of privacy in them? Second, if so, was the appellant's subjective expectation of privacy objectively reasonable such that he has standing to make his s. 8 claim? And third, did the Production Order provide lawful authority for seizing records of historical text messages located in the hands of a service provider?

[8] Le pourvoi dont notre Cour est saisie soulève trois questions. Premièrement, dans le cadre de sa demande fondée sur l'art. 8 de la *Charte*, l'appelant avait-il le droit de s'appuyer sur la thèse de la Couronne suivant laquelle il était l'auteur des Messages textes, afin d'établir son attente subjective au respect de sa vie privée à l'égard de ces messages? Deuxièmement, dans l'affirmative, l'attente subjective de l'appelant au respect de sa vie privée était-elle objectivement raisonnable, de sorte que ce dernier avait qualité pour présenter sa demande fondée sur l'art. 8? Enfin, troisièmement, l'Ordonnance de communication conférait-elle aux policiers l'autorisation légitime de saisir des relevés contenant des messages textes existants se trouvant entre les mains d'un fournisseur de services?

[9] I would answer all three questions in the affirmative. I conclude that an accused mounting a s. 8 claim may ask the court to assume as true any fact that the Crown has alleged or will allege in the prosecution against him in lieu of tendering evidence probative of those same facts in the *voir dire*. In this case, Mr. Jones should have been permitted to rely

[9] Je répondrais par l'affirmative à ces trois questions. Je conclus qu'un accusé qui invoque l'art. 8 peut demander au tribunal de tenir pour avéré tout fait que la Couronne allègue ou entend alléguer dans les poursuites intentées contre lui, au lieu de devoir présenter des éléments de preuve établissant ces mêmes faits lors du voir-dire. En l'espèce, M. Jones

on the Crown allegation that he authored the Text Messages, and his subjective expectation of privacy in the subject matter of the search is accordingly established. Further, it is objectively reasonable for the sender of a text message to expect that a service provider will maintain privacy over the records of his or her text messages stored in its infrastructure. I conclude, however, that the appellant's s. 8 rights were not breached because records of historical text messages were lawfully seized by means of a production order under s. 487.012 of the *Code* (now s. 487.014).

[10] For these reasons and the reasons that follow, I would dismiss the appeal and uphold the validity of the Production Order.

II. Analysis

[11] Section 8 of the *Charter* provides that "[e]veryone has the right to be secure against unreasonable search or seizure." Its basic interpretive structure is well known and consists of two stages. First, the claimant must show that a state act constituted a search or seizure because it invaded his or her reasonable expectation of privacy in the subject matter of the search (*R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 34; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 18). Second, the claimant must show that the search or seizure was itself unreasonable.[1] As a general rule, a *Charter* claimant must prove both the existence of a reasonable expectation of privacy in the relevant subject matter and the unreasonableness of the search or seizure of that subject matter in order to make out a breach of s. 8 (see *R. v. Collins*, [1987] 1 S.C.R. 265).

[1] Warrantless searches are presumed unreasonable in the absence of exigent circumstances (see *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145).

aurait dû être autorisé à s'appuyer sur l'allégation de la Couronne selon laquelle il était l'auteur des Messages textes, et son attente subjective au respect de sa vie privée à l'égard de l'objet de la fouille est par conséquent établie. De plus, il est objectivement raisonnable de la part de l'expéditeur de messages textes de s'attendre à ce qu'un fournisseur de services maintienne la confidentialité des messages en question qu'il conserve dans son infrastructure. Toutefois, j'arrive à la conclusion que les droits garantis à l'appelant par l'art. 8 n'ont pas été violés, étant donné que les relevés contenant les messages textes existants ont été saisis légalement au moyen de l'ordonnance de communication que prévoyait l'art. 487.012 du *Code* (maintenant l'art. 487.014).

[10] Pour les raisons qui précèdent et pour celles énoncées ci-après, je rejetterais le pourvoi et je confirmerais la validité de l'Ordonnance de communication.

II. Analyse

[11] L'article 8 de la *Charte* dispose que « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » La démarche interprétative fondamentale applicable à l'égard de cet article est bien connue et comporte deux étapes. Premièrement, le demandeur doit établir que l'action étatique en cause constituait une fouille, une perquisition ou une saisie en ce qu'elle portait atteinte à ses attentes raisonnables au respect de sa vie privée à l'égard de l'objet de la fouille ou de la perquisition (*R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 34; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 18). Deuxièmement, le demandeur doit démontrer que la fouille, la perquisition ou la saisie elle-même était abusive[1]. En règle générale, pour établir qu'il y a eu violation de l'art. 8, l'auteur d'une demande fondée sur la *Charte* doit prouver à la fois l'existence d'une attente raisonnable au respect de sa vie privée à l'égard de l'objet de la fouille, perquisition ou saisie, ainsi que le caractère abusif de cette fouille, perquisition ou saisie (voir *R. c. Collins*, [1987] 1 R.C.S. 265).

[1] Les fouilles et les perquisitions effectuées sans mandat sont présumées abusives en l'absence de situation d'urgence (voir *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145).

[12] This appeal engages both stages of the s. 8 inquiry.

A. *Does the Appellant Have Standing to Challenge the Production Order?*

[13] I turn first to the question of standing. Does the appellant have a reasonable expectation of privacy in the subject matter of the search? This question has always been answered with regard to the totality of the circumstances of a particular case (see *Edwards*, at para. 31; *R. v. Wong*, [1990] 3 S.C.R. 36, at p. 62). In *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, Cromwell J. explained that, in the context of an informational privacy claim, four lines of inquiry may assist in guiding the required analysis (para. 18):

(1) an examination of the subject matter of the alleged search;

(2) a determination as to whether the claimant had a direct interest in the subject matter;

(3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and

(4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.

(See also *Cole*, at para. 40.)

(1) What Is the Subject Matter of the Search?

[14] First, properly characterizing the subject matter of the search is vital. As explained in *R. v. Marakah*, 2017 SCC 59, [2017] 2 S.C.R. 608, where the state searches records of text messages, it is "the electronic conversation between two or more people" that it seeks to access (para. 19, per McLachlin C.J.). Following *Marakah*, then, the

[12] Le présent pourvoi vise les deux étapes de l'analyse fondée sur l'art. 8.

A. *L'appelant a-t-il qualité pour contester l'Ordonnance de communication?*

[13] Je vais d'abord examiner la question de la qualité pour agir. L'appelant a-t-il une attente raisonnable au respect de sa vie privée à l'égard de l'objet de la fouille? Pour répondre à cette question, les tribunaux tiennent invariablement compte de l'ensemble des circonstances propres à l'affaire dont ils sont saisis (voir *Edwards*, par. 31; *R. c. Wong*, [1990] 3 R.C.S. 36, p. 62). Dans l'arrêt *R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212, le juge Cromwell a expliqué que, dans le contexte d'une revendication du droit à la vie privée d'ordre informationnel, quatre considérations peuvent guider le tribunal dans son analyse (par. 18) :

(1) l'examen de l'objet de la prétendue fouille;

(2) la question de savoir si le demandeur possédait un droit direct à l'égard de l'objet de la fouille;

(3) la question de savoir si le demandeur avait une attente subjective en matière de respect de sa vie privée à l'égard de l'objet de la fouille;

(4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances.

(Voir également l'arrêt *Cole*, par. 40.)

(1) Quel est l'objet de la fouille?

[14] Au départ, il est crucial de qualifier adéquatement l'objet de la fouille. Comme il est expliqué dans *R. c. Marakah*, 2017 CSC 59, [2017] 2 R.C.S. 608, lorsque l'État effectue une fouille visant à recueillir des relevés contenant des messages textes, ce qu'il cherche à consulter c'est « la conversation électronique qui a eu lieu entre deux ou plusieurs

subject matter of the search here is properly characterized as the "electronic conversation" between Mr. Jones and the user of the Gilles phone.

(2) Does the Claimant Have a Direct Interest and Subjective Expectation of Privacy in the Subject Matter of the Search?

[15] In this case, the courts below held that the appellant's s. 8 claim fails at the doorstep because he never established that the Text Messages were indeed *his own*. On appeal, we may readily infer that *if* the appellant authored the Text Messages, then he had a direct interest in their subject matter insofar as they were capable of describing aspects of his biographical core. As a factual matter, it is also uncontested that *if* the appellant authored the Text Messages, then he had a subjective expectation of privacy in records of them stored by the service providers involved in their transmission. Therefore, the real question dictating the result at the second and third steps of the above framework is whether the appellant should have been permitted to rely on the Crown's theory that he was the author of the Text Messages for the purposes of establishing s. 8 standing. As explained below, I would answer that question in the affirmative.

(a) *Should the Appellant Have Been Permitted to Rely on the Crown Theory for the Purposes of Establishing His Subjective Expectation of Privacy in the Text Messages?*

[16] At trial, the Crown tendered the Text Messages as evidence that Mr. Jones offered to transfer a firearm, contrary to s. 99 of the *Criminal Code*. At his *Charter* application challenging their admission, Mr. Jones argued that he need not admit authorship of the impugned evidence in order to mount his s. 8

personnes » (par. 19, la juge en chef McLachlin). Par conséquent, suivant l'arrêt *Marakah*, la « conversation électronique » entre M. Jones et l'utilisateur du téléphone de M. Gilles constitue concrètement l'objet de la fouille.

(2) Le demandeur a-t-il un intérêt direct dans l'objet de la fouille et une attente subjective au respect de sa vie privée à cet égard?

[15] Dans le cas qui nous occupe, les juridictions inférieures ont jugé que la demande de l'appelant fondée sur l'art. 8 échouait dès le départ, parce qu'il n'avait jamais démontré qu'il s'agissait effectivement de *ses propres* Messages textes. Dans le cadre du présent pourvoi, nous pouvons sans aucune hésitation inférer que, *si* l'appelant était l'auteur des Messages textes, il avait donc un intérêt direct dans l'objet de ces messages, étant donné que ceux-ci étaient susceptibles de révéler un ensemble de renseignements biographiques d'ordre personnel à son sujet. De plus, dans les faits, personne ne conteste que, *si* l'appelant était l'auteur des Messages textes, il avait en conséquence une attente subjective au respect de sa vie privée à l'égard des copies de ces messages conservées par les fournisseurs de services ayant participé à leur transmission. Par conséquent, la véritable question — dont la réponse dictera le résultat des deuxième et troisième étapes du cadre d'analyse susmentionné — est celle de savoir si, afin d'établir qu'il avait qualité pour présenter une demande fondée sur l'art. 8, l'appelant pouvait s'appuyer sur la thèse de la Couronne suivant laquelle il était l'auteur des Messages textes. Comme je vais l'expliquer ci-après, je répondrais par l'affirmative à cette question.

a) *L'appelant pouvait-il s'appuyer sur la thèse de la Couronne afin d'établir son attente subjective au respect de sa vie privée à l'égard des Messages textes?*

[16] Au procès, la Couronne a déposé les Messages textes afin d'établir que M. Jones avait, en violation de l'art. 99 du *Code criminel*, offert de céder une arme à feu. Dans le cadre de la demande qu'il a présentée en vertu de la *Charte* pour s'opposer à l'admission en preuve de ces messages,

claim. Instead, he said that for the purposes of establishing his subjective expectation of privacy, he was entitled to rely on the Crown's allegation that he is indeed the author of the Text Messages, without admitting as much.

M. Jones a plaidé qu'il n'était pas tenu d'admettre qu'il était l'auteur des éléments de preuve contestés afin de pouvoir présenter une demande fondée sur l'art. 8. Il a plutôt affirmé que, pour démontrer l'existence de son attente subjective au respect de sa vie privée, il avait le droit de s'appuyer sur l'allégation de la Couronne suivant laquelle il était effectivement l'auteur des Messages textes, sans pour autant admettre le bien-fondé de cette allégation.

[17] In reply, the respondent Crowns state, correctly, that the burden in a *Charter voir dire* is on the claimant, and that discharging that burden typically requires the claimant to present evidence. They say the appellant's s. 8 claim must fail because the accused is not entitled to rely on the federal Crown's theory in the *voir dire*, and "[t]here was no admission of [his] identity as the sender of the texts anywhere in the pre-trial motion record".

[17] À l'encontre de cet argument, les représentants de la Couronne — tant fédérale que provinciale — répliquent à juste titre que, lors d'un voir-dire fondé sur la *Charte*, le fardeau de la preuve incombe au demandeur et que, pour s'acquitter de ce fardeau, ce dernier doit habituellement présenter des éléments de preuve au soutien de ses prétentions. Ils affirment que la demande de l'appelant fondée sur l'art. 8 ne saurait être accueillie, parce que l'accusé n'a pas le droit de s'appuyer sur la thèse de la Couronne fédérale dans le cadre d'un voir-dire, et qu' [TRADUCTION] « [a]ucun aveu [l']identifiant comme étant l'expéditeur des textos ne figurait dans le dossier de la requête présentée avant le procès ».

[18] With respect, I would decline to endorse this position. It effectively creates a catch-22 for an accused in Mr. Jones' shoes: admit that you are the author in the *Charter voir dire*, or forego the ability to challenge admission of the evidence tendered to prove that you are the author in the trial proper.

[18] Avec égards, je ne peux souscrire à cet argument, car il a concrètement pour effet de placer un accusé se trouvant dans la situation de M. Jones devant un dilemme : ou bien il admet être l'auteur des messages textes lors du voir-dire fondé sur la *Charte*, ou bien il renonce à la possibilité de contester, au procès, l'admissibilité des éléments qui sont présentés afin de prouver qu'il en est l'auteur.

[19] Instead, I conclude that Mr. Jones should have been permitted to rely on the Crown's theory that he authored the Text Messages for the purpose of establishing his subjective expectation of privacy in the subject matter of the search. As I explain below, this result coheres with the relatively modest evidentiary foundation required to establish the subjective expectation element in the totality of the circumstances analysis, as well as the principle against self-incrimination.

[19] Je conclus plutôt que M. Jones aurait dû être autorisé à s'appuyer sur la thèse de la Couronne selon laquelle il était l'auteur des Messages textes afin d'établir son attente subjective au respect de sa vie privée à l'égard de l'objet de la fouille. Comme je l'explique ci-après, ce résultat s'accorde avec le fait qu'une preuve relativement minime est requise pour démontrer l'existence de l'attente subjective dans le cadre de l'analyse de l'ensemble des circonstances, ainsi qu'avec le principe protégeant contre l'auto-incrimination.

[20] To begin, the subjective expectation requirement has never been "a high hurdle" (*R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 37). And

[20] Il importe d'abord de préciser que le critère de l'attente subjective n'a jamais été « très exigeant » (*R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579,

for good reason. Overemphasizing the presence or absence of a subjective expectation of privacy cannot be reconciled with the normative nature of the s. 8 inquiry. As Justice Binnie explained in *Tessling*, at para. 42:

> The *subjective* expectation of privacy is important but its absence should not be used too quickly to undermine the protection afforded by s. 8 to the values of a free and democratic society. . . . It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a *subjective* expectation of privacy and thereby forfeits the protection of s. 8. Expectation of privacy is a normative rather than a descriptive standard. [Underlining added.]

[21] The idea here is simple: a *Charter* claimant's subjective belief that Big Brother is watching should not, through the workings of s. 8, be permitted to become a self-fulfilling prophecy. The importance of the subjective expectation element is therefore attenuated in the s. 8 analysis, and the evidentiary foundation required to establish that element is accordingly modest. A subjective expectation of privacy can be presumed or inferred in the circumstances in the absence of the claimant's testimony or admission at the *voir dire* (see *Patrick*, at para. 37; *Tessling*, at para. 38; *Cole*, at para. 43). The modest evidentiary foundation necessary to establish one's subjective expectation of privacy therefore reflects the notion that s. 8's normative import transcends an individual claimant's subjective expectations.

[22] This modest evidentiary foundation also aligns with the practical reality of criminal proceedings. For the defence, it may be a dangerous gambit to call an accused to the stand. That is equally true in a *voir dire*, insofar as an accused's testimony may later be used for incrimination or impeachment purposes or result in tactical disadvantages. Therefore, to the extent that the subjective expectation element can be presumed or inferred in the circumstances, the law has not required an accused to assume the risks of testifying in order to prove that he

par. 37), et ce, pour une bonne raison d'ailleurs. En effet, une insistance trop grande sur la présence ou l'absence d'une attente subjective au respect de la vie privée n'est pas conciliable avec le caractère normatif de l'analyse fondée sur l'art. 8. Ainsi que l'a expliqué le juge Binnie dans l'arrêt *Tessling*, par. 42 :

> L'attente *subjective* en matière de vie privée a son importance, mais il ne faudrait pas utiliser trop rapidement son absence pour écarter la protection des valeurs d'une société libre et démocratique qu'offre l'art. 8. [. . .] Affirmer qu'un particulier qui laisse ses ordures au ramassage n'a pas d'attente raisonnable en matière de vie privée à leur sujet est une chose. Mais c'en est une toute autre de dire qu'une personne qui craint que son téléphone soit sur écoute n'a plus d'attente *subjective* en matière de vie privée et qu'elle ne peut plus de ce fait revendiquer la protection de l'art. 8. L'attente en matière de vie privée est de nature normative et non descriptive. [Je souligne.]

[21] La proposition est simple : on ne saurait laisser la croyance subjective de l'auteur d'une demande fondée sur la *Charte* que « Big Brother » le surveille devenir une prophétie qui se concrétise d'elle-même par l'opération de l'art. 8. L'importance de l'élément relatif à l'attente subjective est par conséquent atténuée dans l'analyse fondée sur l'art. 8, et la preuve requise pour établir cet élément est donc minime. En l'absence de témoignage ou d'aveu du demandeur lors du voir-dire, une telle attente subjective peut être présumée ou inférée eu égard aux circonstances (voir *Patrick*, par. 37; *Tessling*, par. 38; *Cole*, par. 43). La preuve minime qui est requise d'un demandeur donné afin de démontrer son attente subjective au respect de sa vie privée reflète donc l'idée que la portée normative de l'art. 8 transcende les attentes subjectives de ce demandeur.

[22] La preuve minime ainsi requise tient également compte des réalités pratiques des procès criminels. Pour la défense, la décision de faire témoigner l'accusé au procès peut s'avérer périlleuse. Il en va de même lors d'un voir-dire, dans la mesure où son témoignage peut subséquemment être utilisé contre lui pour l'incriminer ou pour attaquer sa crédibilité, ou encore jouer contre lui par la suite sur le plan stratégique. En conséquence, dans la mesure où l'élément relatif à l'attente subjective peut être présumé ou inféré eu égard aux circonstances,

subjectively expected privacy in the subject matter of the search.

[23] The potential risks of testifying or making an admission through counsel in a s. 8 *voir dire* are apparent in Mr. Jones' case. An admission that he authored the Text Messages was tantamount to admitting the charged offence of illegally offering to transfer a firearm. Indeed, at trial, Mr. Jones was convicted because the Crown proved beyond a reasonable doubt that "a series of text messages . . . between Waldron and Jones demonstrate[d] a concerted effort to work together to offer to transfer firearms" (trial judgment, reproduced in A.R., vol. I, at pp. 42-102, at paras. 94 and 95-100). An admission that he was the author was therefore, in practical terms, an admission of both identity and the *actus reus* of the offence.

[24] I am mindful of the rule that evidence in the *voir dire* is not automatically admissible in the trial proper (see *R. v. Gauthier*, [1977] 1 S.C.R. 441, at p. 452; *R. v. Jir*, 2010 BCCA 497, 264 C.C.C. (3d) 64, at para. 10). Still, an admission at the *voir dire* can restrict the permissible scope of defence evidence and submissions at trial. If Mr. Jones admitted authorship of the Text Messages at the *voir dire*, his counsel would have been ethically barred from arguing that someone else had authored the Text Messages in the trial proper. In theory, he could have still held the Crown to its burden to prove authorship of the Text Messages (see, e.g., *R. v. Hurry*, 2002 ABQB 420, 165 C.C.C. (3d) 182, at paras. 1 and 3). But in practice, this presents an accused in Mr. Jones' shoes with difficult tactical decisions. Should he admit authorship in the s. 8 *voir dire* in order to have a chance at holding the state to its *Charter* obligations? Or should he forego a s. 8 claim in order to more rigorously contest the Crown's theory at trial? Perhaps more significantly, should he assume the risk that the admission could

le droit n'oblige pas l'accusé à assumer les risques afférents au fait de témoigner, afin de prouver qu'il s'attendait subjectivement au respect de sa vie privée à l'égard de l'objet de la fouille ou de la perquisition.

[23] Les risques potentiels liés à un témoignage ou à un aveu fait par l'entremise de l'avocat lors d'un voir-dire fondé sur l'art. 8 sont apparents dans le cas de M. Jones. Le fait d'avouer qu'il était l'auteur des Messages textes aurait équivalu à admettre sa culpabilité à l'égard de l'infraction reprochée, soit le fait d'avoir illégalement offert de céder une arme à feu. D'ailleurs, au procès, M. Jones a été déclaré coupable parce que le ministère public a prouvé hors de tout doute raisonnable [TRADUCTION] « qu'une série de messages textes échangés [. . .] entre MM. Waldron et Jones démontraient des efforts concertés de leur part en vue de collaborer afin d'offrir de céder des armes à feu » (jugement de première instance, reproduit au d.a., vol. I, p. 42-102, par. 94 et 95-100). Un aveu de M. Jones reconnaissant qu'il était l'auteur des Messages textes aurait donc constitué, en pratique, un aveu à la fois sur la question de l'identité et sur celle de l'*actus reus* de l'infraction.

[24] Je suis consciente de la règle selon laquelle la preuve présentée au voir-dire n'est pas automatiquement admissible lors du procès proprement dit (voir *R. c. Gauthier*, [1977] 1 R.C.S. 441, p. 452; *R. c. Jir*, 2010 BCCA 497, 264 C.C.C. (3d) 64, par. 10). Néanmoins, un aveu fait lors du voir-dire peut avoir pour effet de limiter l'étendue de la preuve et des arguments que la défense sera admise à présenter au procès. Si M. Jones avait avoué au voir-dire être l'auteur des Messages textes, son avocat n'aurait pas été autorisé, sur le plan éthique, à plaider au procès proprement dit que quelqu'un d'autre en était l'auteur. En théorie, il aurait toujours pu obliger la Couronne à s'acquitter du fardeau qui lui incombait, à savoir prouver l'identité de l'auteur des Messages textes (voir, p. ex., *R. c. Hurry*, 2002 ABQB 420, 165 C.C.C. (3d) 182, par. 1 et 3). Mais, en pratique, un accusé qui se trouve dans la situation de M. Jones est aux prises avec des décisions tactiques difficiles. Devrait-il, lors du voir-dire fondé sur l'art. 8, reconnaître qu'il est l'auteur des Messages textes afin de se ménager la possibilité d'obliger l'État à

be used by the Crown for inculpatory or impeachment purposes?[2]

[25] The federal Crown submits these choices follow from the fact that the *Charter* is not a "tactical Bill of Rights" which permits the accused to have his cake and eat it too. With respect, I see the matter differently for three reasons.

[26] First, the Crown's argument on this point cuts both ways. As the intervener Criminal Lawyers' Association of Ontario argues, the Crown should not be permitted to say there is sufficient evidence proving Mr. Jones' authorship of the messages beyond a reasonable doubt at trial, but argue that he has not discharged his burden on the balance of probabilities in the *voir dire*. The Crown is right to argue that it is the *accused's s. 8 motion*. But that motion arises within the *Crown's prosecution*. And it is the Crown, as a quasi-minister of justice, that is charged with ensuring the overall fairness of that prosecution. Therefore, as between the accused and the Crown, it is more fitting that the Crown be restrained from adopting inconsistent positions.

respecter les obligations qui lui incombent en vertu de la *Charte*? Devrait-il plutôt renoncer à la possibilité d'invoquer l'art. 8 afin de pouvoir contester plus rigoureusement la thèse du ministère public au procès? Ou bien — considération encore plus lourde de conséquences — devrait-il courir le risque que la Couronne se serve de son aveu en vue d'établir sa culpabilité ou de contester sa crédibilité[2]?

[25] La Couronne fédérale soutient que ces choix découlent du fait que la *Charte* ne constitue pas une [TRADUCTION] « déclaration des droits d'ordre tactique » qui permet à l'accusé de gagner sur tous les tableaux. Soit dit en tout respect, je vois les choses différemment, et ce, pour trois raisons.

[26] Premièrement, l'argument de la Couronne sur ce point joue dans les deux sens. En effet, comme l'affirme l'intervenante la Criminal Lawyers' Association of Ontario, on ne saurait permettre à la Couronne, d'une part, de prétendre au procès qu'il y a suffisamment d'éléments démontrant hors de tout doute raisonnable que M. Jones était l'auteur des messages, mais, d'autre part, d'affirmer que ce dernier ne s'est pas acquitté, selon la prépondérance des probabilités, du fardeau de preuve qui lui incombait lors du voir-dire. La Couronne a raison de soutenir qu'il s'agit *d'une requête présentée par l'accusé en vertu de l'art. 8*. Mais la présentation de cette requête s'inscrit dans la foulée *des poursuites intentées par la Couronne.* Et c'est cette dernière, en qualité de quasi-ministre de la Justice, qui est chargée de veiller à l'équité générale de ces poursuites. Par conséquent, il convient davantage d'empêcher la Couronne — plutôt que l'accusé — d'adopter des positions incompatibles.

[2] In posing this question, I note that this Court has not ruled on whether a *Charter* claimant's testimony in a s. 8 *voir dire* is subject to the protections against self-incrimination provided by s. 13 of the *Charter*. Nor is this the proper case to do so. However, it may follow from this Court's decisions in *R. v. Henry*, 2005 SCC 76, [2005] 3 S.C.R. 609, and *R. v. Nedelcu*, 2012 SCC 59, [2012] 3 S.C.R. 311, that because the accused is not a compellable witness at his own s. 8 *voir dire*, his evidence could subsequently be used to cross-examine him for both incrimination and impeachment purposes. To that extent, Mr. Jones would be reluctant to admit he authored the Text Messages because he was worried about potentially incriminating himself.

[2] Je tiens à souligner, en posant cette question, que notre Cour ne s'est pas encore prononcée sur la question de savoir si la personne qui témoigne lors d'un voir-dire tenu à l'égard de la demande qu'elle présente en vertu de l'art. 8 de la *Charte* bénéficie des garanties contre l'auto-incrimination prévues à l'art. 13 de ce même texte. Et il ne s'agit pas non plus d'une affaire se prêtant à un tel examen. Toutefois, il découle peut-être des arrêts de notre Cour *R. c. Henry*, 2005 CSC 76, [2005] 3 R.C.S. 609, et *R. c. Nedelcu*, 2012 CSC 59, [2012] 3 R.C.S. 311, que, comme un accusé ne peut être contraint à témoigner lors de son propre voir-dire fondé sur l'art. 8, son témoignage pourrait être utilisé ultérieurement pour le contre-interroger tant en vue de l'incriminer que d'attaquer sa crédibilité. Pour cette raison, M. Jones était hésitant à admettre qu'il était l'auteur des Messages textes, de crainte que cela puisse éventuellement l'incriminer.

[27] Second — and on a more practical note — I respectfully reject the Crown's argument that allowing the accused to rely on the Crown's theory in his *Charter* application would be procedurally inefficient because the accused would not be tactically bound to his position at the *voir dire*. In this case, the trial judge had the benefit of at least the following on the s. 8 *Charter* claim:

(i) The Information to Obtain the Production Order listing Mr. Jones as the user of the cellphone from which the Text Messages were sent; and

(ii) A submission from the Crown that "the evidence is very clear that it is [Mr. Jones' and Mr. Waldron's] communication, but they haven't said that".

[28] At first instance, the s. 8 claim turned on the novel legal question that is now before this Court. It was not a factually driven dispute. In that situation, permitting the accused to rely on the Crown's theory is more efficient than requiring the accused to call circumstantial evidence in an attempt to ground his desired inference.

[29] Third, requiring an accused to admit Crown allegations in order to have a shot at holding the state to its constitutional obligations under s. 8 sits uneasily alongside the principle against self-incrimination. The principle against self-incrimination is a principle of fundamental justice under s. 7 of the *Charter* and provides a "general organizing principle of criminal law from which particular rules can be derived" (*R. v. Hart*, 2014 SCC 52, [2014] 2 S.C.R. 544, at para. 123, quoting *R. v. Jones*, [1994] 2 S.C.R. 229, at p. 249). It reflects the basic tenet that "the Crown must establish a 'case to meet' before there can be any expectation that the accused should respond"

[27] Deuxièmement — et d'un point de vue plus pratique —, je dois avec égards rejeter l'argument de la Couronne suivant lequel il serait inefficace au plan procédural d'autoriser l'accusé à s'appuyer sur la thèse de la Couronne dans sa demande fondée sur la *Charte*, étant donné que ce dernier ne serait pas tenu, sur le plan tactique, de s'en tenir à la position qu'il a avancée au voir-dire. Dans le cas qui nous occupe, la juge du procès avait l'avantage d'avoir en mains à tout le moins les éléments suivants lors de l'examen de la demande fondée sur l'art. 8 de la *Charte* :

(i) la dénonciation qui avait été déposée en vue d'obtenir l'Ordonnance de communication et qui mentionnait que M. Jones était l'utilisateur du téléphone cellulaire à partir duquel les Messages textes avaient été envoyés;

(ii) la prétention de la Couronne selon laquelle [TRADUCTION] « il ressort très clairement de la preuve qu'il s'agit de communications entre [M. Jones et M. Waldron], mais ils n'ont pas dit que c'était le cas ».

[28] En première instance, la demande fondée sur l'art. 8 portait sur la nouvelle question de droit dont notre Cour est maintenant saisie. Il ne s'agissait pas d'un litige axé sur les faits. Dans un tel cas, il est plus efficace de permettre à l'accusé de s'appuyer sur la thèse de la Couronne que de l'obliger à présenter des éléments de preuve circonstanciels afin de tenter d'étayer l'inférence qu'il souhaite qu'on en tire.

[29] Troisièmement, obliger l'accusé à admettre le bien-fondé des allégations de la Couronne afin d'avoir la possibilité d'obliger l'État à respecter les obligations constitutionnelles qui lui incombent en vertu de l'art. 8 s'accorde mal avec la règle protégeant contre l'auto-incrimination. Cette règle est un principe de justice fondamentale consacré par l'art. 7 de la *Charte*, constituant un « principe directeur général de droit criminel, dont il est possible de tirer des règles particulières » (*R. c. Hart*, 2014 CSC 52, [2014] 2 R.C.S. 544, par. 123, citant l'arrêt *R. c. Jones*, [1994] 2 R.C.S. 229, p. 249). Elle reflète le précepte fondamental voulant que « le ministère

(*R. v. White*, [1999] 2 S.C.R. 417, at para. 41). Like s. 8, it is grounded in the value "placed by Canadian society upon individual privacy, personal autonomy and dignity" (*Hart*, at para. 123, citing *White*, at para. 43). However, requiring an accused to effectively admit Crown allegations as a pre-requisite to making full answer and defence through bringing a s. 8 *Charter* challenge creates a tension with the principle against self-incrimination. Indeed, this tension may well have resulted in Mr. Jones' decision not to lead evidence going to his subjective expectation of privacy.

[30] In my view, however, this tension need not arise. Although the principle against self-incrimination is not a free-standing legal protection, it is to be considered in fashioning legal rules in the development of the common law and *Charter* law (see, e.g., *Hart*, at para. 123; *White*, at para. 45). As Iacobucci J. explained in *White*, at para. 45:

> The principle against self-incrimination demands different things at different times, with the task in every case being to determine exactly what the principle demands, if anything, within the particular context at issue.

[31] What, if anything, does the principle demand in the instant context? It is clear that, to the extent possible, the elements of s. 8 — which in itself provides a fundamental principle of justice — should be informed by, and reconciled with, the principle against self-incrimination.

[32] In my view, that is best accomplished by concluding that counsel for a s. 8 applicant may ask the court to assume as true for s. 8 purposes any fact that the Crown has alleged or will allege in the prosecution against him. In other words, where the alleged

public établisse une "preuve complète" avant que surgisse une attente de réponse de la part de l'accusé » (*R. c. White*, [1999] 2 R.C.S. 417, par. 41). À l'instar de l'art. 8, cette règle repose sur « la valeur qu'attribue la société canadienne à la vie privée, à l'autonomie personnelle et à la dignité » (*Hart*, par. 123, citant l'arrêt *White*, par. 43). Cependant, le fait d'obliger un accusé à reconnaître effectivement le bien-fondé des allégations de la Couronne avant de lui accorder la possibilité de présenter une défense pleine et entière en soumettant une contestation fondée sur l'art. 8 de la *Charte* est source de tension, car une telle obligation va à l'encontre de la règle protégeant contre l'auto-incrimination. D'ailleurs, cette tension peut fort bien être à l'origine de la décision de M. Jones de ne pas présenter de preuve au sujet de son attente subjective au respect de sa vie privée.

[30] Je suis toutefois d'avis qu'une telle tension n'est pas nécessaire. Bien que la règle protégeant contre l'auto-incrimination ne soit pas une garantie juridique autonome, elle doit être prise en compte dans l'élaboration des règles de droit dans le cadre de l'évolution de la common law et du droit relatif à la *Charte* (voir, p. ex., *Hart*, par. 123; *White*, par. 45). Comme l'a expliqué le juge Iacobucci dans l'arrêt *White*, par. 45 :

> Le principe interdisant l'auto-incrimination exige différentes choses à différents moments, la tâche dans chaque affaire étant de déterminer avec précision ce que le principe exige, s'il y a lieu, dans le contexte particulier en cause.

[31] Quelles sont les exigences, s'il en est, découlant de cette règle dans le présent contexte? Il est évident que, dans la mesure du possible, les éléments de l'art. 8 — lequel constitue lui-même un principe de justice fondamentale — doivent tenir compte de la règle protégeant contre l'auto-incrimination et être compatibles avec celle-ci.

[32] À mon avis, la meilleure façon d'y parvenir consiste à conclure que l'avocat de l'auteur d'une demande fondée sur l'art. 8 peut demander au tribunal de tenir pour avéré tout fait que la Couronne allègue ou entend alléguer dans les poursuites intentées

Crown facts, if taken to be true, would establish certain elements of the applicant's s. 8 claim, he or she need not tender additional evidence probative of those facts in order to make out those same elements. Although the entirety of the facts and the Crown theory may not be apparent at the time of the *voir dire*, the court may infer it from the nature of the charges. Alternatively, the court may encourage prosecutors to be forthright in regards to their theory.

[33] The preceding lays out an exception to the rule that a *Charter* applicant "bears the burden of persuading the court that [his] *Charter* rights or freedoms have been infringed or denied" (*Collins*, at p. 277). Mr. Jones is entitled to rely on this exception because, as explained above, Ontario Crown counsel tendered the Text Messages to prove that he was the author of their inculpatory contents, and admitted in the *voir dire* that the evidence was "very clear" in that respect. Pursuant to the Crown's theory, then, he should have been presumed to be the author of the Text Messages for the purposes of his s. 8 application.

[34] In the instant circumstances, it follows that Mr. Jones subjectively expected privacy in records of his electronic conversation found in the service provider's infrastructure. As the Court of Appeal correctly noted, text messages are private communications. This is not in dispute. Further, as the application judge found, Mr. Jones and his co-accused used third-party names so as to "avoid detection or association with" the Text Messages (application judgment, reproduced in A.R., vol. I, at pp. 1-41, at para. 31). This suggests they intended their communications to remain private. Accordingly, we may infer that Mr. Jones had a subjective expectation of privacy in the subject matter of the search.

contre son client. En d'autres mots, lorsque les faits allégués par la Couronne, s'ils sont tenus pour avérés, établiraient certains aspects de la demande fondée sur l'art. 8, l'auteur de cette demande n'a pas à présenter des éléments de preuve additionnels pour prouver ces aspects. Bien que l'ensemble des faits ainsi que la thèse de la Couronne ne ressortent peut-être pas de manière évidente au moment du voir-dire, il est possible au tribunal de les inférer de la nature des accusations. Subsidiairement, le tribunal peut encourager les poursuivants à exposer clairement leur thèse.

[33] Ce qui précède constitue une exception au principe suivant lequel l'auteur d'une demande fondée sur la *Charte* « a la charge de persuader la cour de la violation ou de la négation des droits ou libertés que lui confère la *Charte* » (*Collins*, p. 277). Monsieur Jones a le droit d'invoquer cette exception parce que, comme je l'ai expliqué plus tôt, l'avocat de la Couronne de l'Ontario a soumis les Messages textes pour établir que M. Jones en était l'auteur, et il a reconnu au voir-dire que la preuve était [TRADUCTION] « très claire » à cet égard. Par conséquent, conformément à la thèse de la Couronne, M. Jones était l'auteur présumé des Messages textes lors de l'examen de sa demande fondée sur l'art. 8.

[34] Dans les circonstances de l'espèce, il s'ensuit que M. Jones s'attendait subjectivement à ce que l'on respecte son droit à la vie privée relativement aux copies de sa conversation électronique se trouvant dans l'infrastructure du fournisseur de services. Comme l'a souligné à juste titre la Cour d'appel, les messages textes constituent des communications privées. Cela n'est pas contesté. De plus, comme a conclu la juge saisie de la demande, M. Jones et son coaccusé se sont servis de noms de tiers pour [TRADUCTION] « éviter d'être repérés ou d'être associés » aux Messages textes (jugement sur la demande, reproduit au d.a., vol. I, p. 1-41, par. 31). Cela tend à indiquer qu'ils entendaient que leurs communications demeurent privées. Par conséquent, il est possible d'en inférer que M. Jones avait une attente subjective au respect de sa vie privée relativement à l'objet de la fouille.

(3) Is the Appellant's Subjective Expectation of Privacy Objectively Reasonable?

[35] Having determined that Mr. Jones had a subjective expectation of privacy in the subject matter of the search, the question then becomes whether that expectation is an objectively reasonable one. To be clear, the issue here is whether the sender of a text message has a reasonable expectation of privacy in records of that message stored in the service provider's infrastructure. The further question of whether or not it is reasonable for that expectation to persist when the information is in the hands of the intended recipient is the focus of the *Marakah* appeal.

[36] The application judge held that Mr. Jones did not have a reasonable expectation of privacy in the Text Messages, and the majority of the Court of Appeal upheld her decision. The arguments in support of their respective holdings can be distilled into two lines of thought. The first is a general proposition that the sender of a text message does not have a reasonable expectation of privacy in records of that message in the hands of the service provider because he voluntarily relinquished control over the message when he sent it. The second points to the rest of the totality of the circumstances in this case, namely that:

(i) the appellant was not a party to a confidentiality agreement with Telus; and

(ii) the Production Order and attendant seizure targeted a Telus account in the name of a third party.

[37] In my view, these arguments are no answer to Mr. Jones' claim for s. 8 standing. As I see it, it was reasonable for him to expect that the Text Messages he sent would not be shared by a service provider

(3) L'attente subjective de l'appelant au respect de sa vie privée est-elle objectivement raisonnable?

[35] Vu ma conclusion selon laquelle M. Jones avait une attente subjective au respect de sa vie privée relativement à l'objet de la fouille, il s'agit maintenant de décider si cette attente était objectivement raisonnable. En clair, la question à laquelle il faut répondre en l'espèce est celle de savoir si l'expéditeur d'un message texte possède une attente raisonnable au respect de sa vie privée à l'égard des copies de ce message texte conservées dans l'infrastructure du fournisseur de services. L'autre question qui se pose — c'est-à-dire celle de savoir si cette attente demeure raisonnable lorsque les renseignements se trouvent entre les mains du destinataire visé — est la question en litige dans le pourvoi *Marakah*.

[36] La juge saisie de la demande a conclu que M. Jones n'avait pas d'attente raisonnable au respect de sa vie privée relativement aux Messages textes, et la Cour d'appel a confirmé cette décision à la majorité. Les arguments étayant leur décision respective peuvent être résumés en deux raisonnements distincts. Le premier repose sur la proposition générale voulant que l'expéditeur d'un message texte ne possède pas d'attente raisonnable au respect de sa vie privée relativement aux copies de ce message lorsque celui-ci se trouve entre les mains du fournisseur de services, pour le motif qu'il a volontairement renoncé à la maîtrise de ce message lorsqu'il l'a envoyé. Le second raisonnement met l'accent sur l'ensemble des circonstances de l'espèce, à savoir :

(i) l'appelant n'était pas partie à une entente de confidentialité avec Telus;

(ii) l'Ordonnance de communication et la saisie qui en a découlé visaient un compte Telus enregistré au nom d'un tiers.

[37] À mon avis, ces arguments ne répondent pas à la prétention de M. Jones suivant laquelle il a la qualité requise pour présenter une demande fondée sur l'art. 8. À mon sens, il était raisonnable de sa

with any parties other than the intended recipient. And, as explained below, neither the absence of a contractual policy, nor the fact that the Production Order targeted a third party, deprives him of that protection.

(a) *Does the Sender of a Text Message Have a Reasonable Expectation of Privacy in Its Informational Contents in the Hands of a Service Provider?*

[38] Like all *Charter* rights, s. 8 demands a purposive interpretation (*R. v. Big M Drug Mart Ltd.*, [1985] 1 S.C.R. 295, at p. 344). It is therefore helpful to begin by recalling its essential purpose. Section 8 protects an individual's reasonable expectation of privacy — his or her reasonable "right to be [left] alone by other people" (*Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 159). As understood by this Court, personal privacy is vital to an individual's dignity, autonomy, and personal growth (*R. v. Golden*, 2001 SCC 83, [2001] 3 S.C.R. 679, at paras. 89-90; *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 427-28; *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 292; *Spencer*, at para. 48). The protection of personal privacy is accordingly a basic prerequisite to the flourishing of a free and healthy democracy.

[39] In the context of informational privacy, specifically, this Court has long recognized that "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" (*Dyment*, at p. 429, quoted in *Spencer*, at para. 40). The concern here is informational self-determination. Just as individuals may choose to be left alone in their own homes by closing the door on the state and reasonably expect privacy, they may choose to divulge certain information for a limited purpose, or to a limited class of persons, and nonetheless retain a reasonable expectation of privacy,

part de s'attendre à ce que le fournisseur de services ne communiquerait à personne d'autre qu'au destinataire visé les Messages textes qu'il envoyait. De plus, comme je l'expliquerai plus loin, ni l'absence de politique de confidentialité de nature contractuelle ni le fait que l'Ordonnance de communication visait un tiers ne le privent de cette protection.

a) *L'expéditeur d'un message texte a-t-il une attente raisonnable au respect de sa vie privée relativement au contenu informationnel de ce message texte lorsqu'il se trouve entre les mains d'un fournisseur de services?*

[38] Comme tous les autres droits garantis par la *Charte*, l'art. 8 commande une interprétation téléologique (*R. c. Big M Drug Mart Ltd.*, [1985] 1 R.C.S. 295, p. 344). Il est donc utile de commencer en rappelant la raison d'être fondamentale de cette disposition. L'article 8 protège l'attente raisonnable d'une personne au respect de sa vie privée, c'est-à-dire son droit raisonnable « de ne pas être importuné[e] par autrui » (*Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 159). Suivant l'interprétation qu'en a donnée notre Cour, le respect de la vie privée d'un individu est essentiel pour assurer la dignité, l'autonomie et la croissance personnelle de celui-ci (*R. c. Golden*, 2001 CSC 83, [2001] 3 R.C.S. 679, par. 89-90; *R. c. Dyment*, [1988] 2 R.C.S. 417, p. 427-428; *R. c. Plant*, [1993] 3 R.C.S. 281, p. 292; *Spencer*, par. 48). La protection de la vie privée des individus est par conséquent une condition préalable essentielle à l'épanouissement d'une démocratie libre et en santé.

[39] Dans le contexte de l'intimité informationnelle, en particulier, notre Cour reconnaît depuis longtemps que « l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend » (*Dyment*, p. 429, cité dans *Spencer*, par. 40). La préoccupation en cause dans la présente affaire est l'autodétermination informationnelle. Tout comme une personne peut choisir de ne pas être importunée par autrui à son domicile en fermant sa porte aux représentants de l'État et raisonnablement s'attendre au respect de sa vie privée, cette même personne

depending on the circumstances. When it comes to s. 8, protecting such choices is essential.

[40] In the totality of the circumstances analysis, a s. 8 claimant's direct *control* over the subject matter of the privacy claim and his or her ability to directly regulate *access* thereto have figured prominently in the analysis (*Edwards*, at para. 31; *Patrick*, at para. 27; *Tessling*, at para. 32; *Cole*, at paras. 45-58). For example, relinquishing control over physical subject matter by putting it out for garbage collection, or by discarding it into a garbage can, may reasonably reflect a meaningful choice to abandon one's privacy interest in that subject matter (see, e.g., *Patrick*; *R. v. Stillman*, [1997] 1 S.C.R. 607). On the other hand, keeping financial documents in a locked safe may reflect a choice to keep the information private (*R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227). The control and access factors have also been particularly salient in territorial privacy cases. As suggested above, land owners and tenants have a practical ability to exclude visitors from their territory and maintain a choice to be left alone by controlling access to their domicile (*Patrick*; *Edwards*; *R. v. Pugliese* (1992), 71 C.C.C. (3d) 295 (Ont. C.A.)). In these traditional circumstances, it is meaningful to speak of direct control, access and choice in the same breath, since relinquishing control and giving others access to the subject matter of a privacy claim may indicate that it is unreasonable to expect privacy in that subject matter.

peut pareillement choisir de divulguer certains renseignements soit pour une fin précise, soit encore à une catégorie restreinte de personnes, et néanmoins conserver une attente raisonnable au respect de sa vie privée, selon les circonstances. Lorsque l'art. 8 est en jeu, il est essentiel de protéger la faculté de faire ces choix.

[40] Le *contrôle* direct qu'exerce l'auteur d'une demande fondée sur l'art. 8 sur l'objet de sa revendication du droit au respect de sa vie privée, ainsi que la capacité de cette personne de régir directement l'*accès* à cet objet, sont des facteurs qui ont joué un rôle de premier plan dans l'analyse de l'ensemble des circonstances (*Edwards*, par. 31; *Patrick*, par. 27; *Tessling*, par. 32; *Cole*, par. 45-58). Par exemple, le fait qu'une personne ait renoncé au contrôle de l'objet physique visé par la fouille, par exemple en le déposant pour qu'il soit ramassé au bord du chemin lors de la collecte des ordures, ou encore en le jetant dans une poubelle, peut raisonnablement témoigner de son choix réfléchi de renoncer au respect de son droit à la vie privée à l'égard de cet objet (voir, p. ex., *Patrick*; *R. c. Stillman*, [1997] 1 R.C.S. 607). En revanche, le fait que des documents financiers soient conservés dans un coffre-fort peut être une indication de la décision de préserver le caractère privé de l'information qu'ils contiennent (*R. c. Law*, 2002 CSC 10, [2002] 1 R.C.S. 227). Ces facteurs — le contrôle et l'accès — ont également joué un rôle particulièrement important dans les affaires relatives à l'intimité territoriale. Comme il a été mentionné plus tôt, les propriétaires et locataires d'immeubles possèdent la faculté concrète d'exclure les visiteurs de leur territoire et de choisir de ne pas y être importunés en limitant l'accès à leur domicile (*Patrick*; *Edwards*; *R. c. Pugliese* (1992), 71 C.C.C. (3d) 295 (C.A. Ont.)). Dans de telles situations, il est logique d'invoquer en même temps les notions de contrôle direct, d'accès et de choix, car le fait qu'une personne renonce à l'exercice du contrôle sur l'objet de sa revendication du droit au respect de sa vie privée et qu'elle donne à autrui accès à cet objet peut indiquer qu'il n'est pas raisonnable dans un tel cas que cette personne s'attende au respect de sa vie privée à cet égard.

[41] However, as this Court recognized in *Spencer* and *TELUS*, control and access are not all or nothing concepts.

[42] In *Spencer*, police requested subscriber information associated with a particular Internet Protocol ("IP") address from an Internet service provider. An IP address leaves a trail of "digital breadcrumbs" with the service provider (see S. Magotiaux, "Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence" (2015), 71 *S.C.L.R.* (2d) 501, at p. 502). Those breadcrumbs are capable of revealing a history of one's private activity on the Internet (see *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, at para. 36). But once left in the hands of the service provider, they are out of the Internet user's direct control. The Court in *Spencer* nevertheless recognized that Mr. Spencer had a reasonable expectation of privacy in the subject matter of the search, even if an Internet "user cannot fully control or even necessarily be aware of who may observe a pattern of online activity" (para. 46). In doing so, the Court relied in part on the legislative framework in the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*"):

> Given that the purpose of *PIPEDA* is to establish rules governing, among other things, disclosure "of personal information in a manner that recognizes the right of *privacy* of individuals with respect to their personal information" . . . it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent. [Underlining added.]

(*Spencer*, at para. 62)

[43] Similarly, in *TELUS*, a plurality of the Court recognized that:

[41] Toutefois, comme l'a reconnu notre Cour dans les arrêts *Spencer* et *TELUS*, le contrôle et l'accès ne sont pas des concepts absolus.

[42] Dans *Spencer*, les policiers avaient obtenu d'un fournisseur de services Internet des renseignements relatifs à l'abonné à qui appartenait une adresse de protocole Internet (« IP ») particulière. Or, une adresse IP laisse des traces sous forme de [TRADUCTION] « fragments numériques » auprès du fournisseur de services (voir S. Magotiaux, « Out of Sync : Section 8 and Technological Advancement in Supreme Court Jurisprudence » (2015), 71 *S.C.L.R.* (2d) 501, p. 502). Ces fragments sont susceptibles de révéler l'historique des activités privées d'une personne sur Internet (voir *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, par. 36). Cependant, une fois qu'ils se trouvent entre les mains du fournisseur de services, ces fragments échappent au contrôle direct de l'internaute. Dans l'arrêt *Spencer*, notre Cour a néanmoins reconnu que M. Spencer avait une attente raisonnable au respect de sa vie privée à l'égard de l'objet de la fouille, et ce, même si un internaute « n'est pas en mesure d'exercer un contrôle total à l'égard de la personne qui peut observer le profil de ses activités en ligne et [. . .] n'est pas toujours informé de l'identité de celle-ci » (par. 46). La Cour a tiré cette conclusion en s'appuyant en partie sur le cadre législatif établi par la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 (« *LPRPDE* ») :

> Puisque la *LPRPDE* a pour objet de fixer des règles régissant, entre autres, la communication de « renseignements personnels d'une manière qui tient compte du droit des individus *à la vie privée* à l'égard des renseignements personnels qui les concernent » [. . .] il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou qu'elle n'écarte pas l'interdiction générale prévue par la *LPRPDE* quant à la communication de renseignements personnels sans le consentement de l'intéressé. [Je souligne.]

(*Spencer*, par. 62)

[43] De même, dans l'arrêt *TELUS*, une pluralité de juges de notre Cour ont reconnu ce qui suit :

. . . 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 . . . . [para. 41]

[44] *TELUS* implicitly acknowledges that, as a normative matter, it is reasonable to expect a service provider to keep information private where its receipt and retention of such information is incidental to its role of delivering private communications to the intended recipient. That is intuitive. One would not reasonably expect the service provider to share his text messages with an unintended recipient, or post them publicly for the world to see.

[45] This case is akin to *Spencer* and *TELUS* in the sense that Mr. Jones' decision to message Mr. Waldron necessarily leaves a trail of digital breadcrumbs with Telus. However, as in *Spencer* and *TELUS*, this does not eliminate Mr. Jones' reasonable expectation that a service provider would keep the Text Messages private. Like the service provider in *Spencer*, the service provider here is subject to the provisions of *PIPEDA*, which strictly limit its ability to disclose information (see, e.g., ss. 3, 5(3) and 7 of *PIPEDA*). As *Spencer* demonstrates, those limitations operate regardless of whether or not the target of the search is a subscriber of that particular service provider. Here, as in *Spencer* and *TELUS*, the only way to retain control over the subject matter of the search vis-à-vis the service provider was to make no use of its services at all. That choice is not a meaningful one. Focusing on the fact that Mr. Jones relinquished direct control vis-à-vis the service provider is accordingly difficult to reconcile with a purposive approach to s. 8. Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives. I therefore conclude that the sender of a text message retains a reasonable expectation of privacy in records of text messages stored in a service provider's infrastructure notwithstanding that he relinquished direct control over

. . . les fournisseurs de services de télécommunications ne sont que des tiers qui transmettent des communications privées à titre d'« agents » et [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 . . . [par. 41]

[44] L'arrêt *TELUS* reconnaît implicitement que, sur le plan normatif, il est raisonnable de s'attendre à ce qu'un fournisseur de services protège le caractère privé de l'information qui lui est confiée, dans les cas où la réception et la conservation de cette information constituent un aspect accessoire de son rôle consistant à acheminer des communications privées au destinataire visé. Cette conclusion a un caractère intuitif. En effet, il ne serait pas raisonnable de s'attendre à ce qu'un fournisseur de services communique des messages textes à un destinataire non visé ou qu'il les mette à la disposition du monde entier.

[45] La présente espèce s'apparente aux affaires *Spencer* et *TELUS* en ce sens que la décision de M. Jones d'envoyer des messages textes à M. Waldron a nécessairement laissé des traces sous forme de fragments numériques chez Telus. Toutefois, tout comme dans *Spencer* et *TELUS*, cette situation n'a pas pour effet d'empêcher M. Jones de s'attendre raisonnablement à ce que le fournisseur de services protège le caractère privé de ses Messages textes. À l'instar du fournisseur de services en cause dans *Spencer*, le fournisseur de services concerné en l'espèce est assujetti aux dispositions de la *LPRPDE*, lesquelles limitent strictement sa capacité de communiquer des renseignements (voir, p. ex., les art. 3 et 7, ainsi que le par. 5(3) de la *LPRPDE*). Comme le démontre l'arrêt *Spencer*, ces restrictions s'appliquent, peu importe que la cible de la fouille soit ou non un abonné du fournisseur de services concerné. En l'espèce, tout comme dans les affaires *Spencer* et *TELUS*, la seule façon qu'avait l'intéressé de conserver, vis-à-vis du fournisseur de services, un contrôle sur l'objet de la fouille, était de s'abstenir complètement d'utiliser ses services. Il ne s'agit évidemment pas là d'un véritable choix. Mettre l'accent sur la renonciation par M. Jones à exercer un contrôle direct sur le fournisseur de services est par conséquent difficilement conciliable

those messages. This result comports with contemporary social norms and a purposive approach to s. 8. It also comports with the purpose of *PIPEDA*, and the approaches adopted by this Court in *Spencer* and *TELUS*.

avec une interprétation téléologique de l'art. 8. Les Canadiens n'ont pas à vivre en reclus du monde numérique afin de pouvoir conserver un semblant de vie privée. En conséquence, je conclus que l'expéditeur d'un message texte conserve une attente raisonnable au respect de sa vie privée à l'égard des copies des messages textes conservées dans l'infrastructure du fournisseur de services, malgré le fait qu'il ait renoncé à exercer un contrôle direct sur ces messages. Cette conclusion s'accorde avec les normes sociales actuelles, ainsi qu'avec une interprétation téléologique de l'art. 8. Elle se concilie également avec l'objet de la *LPRPDE* et avec la démarche retenue par notre Cour dans les arrêts *Spencer* et *TELUS*.

[46] The next question is whether that expectation is rendered unreasonable in the appellant's case because he had no confidentiality agreement with Telus and the Production Order and attendant seizure targeted a Telus account in the name of a third party. As the Ontario Crown concedes, that the Text Messages were sent from a phone registered to Mr. Jones' spouse does not detract from his reasonable expectation of privacy.

[46] La prochaine question qu'il faut trancher consiste à se demander si cette attente devient déraisonnable en ce qui concerne l'appelant, du fait que ce dernier n'avait pas signé d'entente de confidentialité avec Telus et que l'Ordonnance de communication et la saisie en découlant visaient un compte Telus enregistré au nom d'un tiers. Comme le concède la Couronne de l'Ontario, le fait que les Messages textes aient été envoyés à partir d'un téléphone enregistré au nom de la conjointe de M. Jones ne diminue pas l'attente raisonnable de ce dernier au respect de sa vie privée.

(b) *The Absence of a Confidentiality Agreement Does Not Defeat Mr. Jones' Standing Claim*

b) *L'absence d'entente de confidentialité ne fait pas échec à la prétention de M. Jones selon laquelle il a qualité pour agir*

[47] The application judge's finding that "[t]here is nothing to suggest that Telus was contractually bound to keep any of the records confidential" militated against the appellant's s. 8 standing (para. 31). I agree that this factor operates against the appellant. But in my view, it does so only to a limited extent. When considered in light of the totality of the circumstances, it does not defeat the appellant's claim for standing.

[47] La conclusion de la juge saisie de la demande suivant laquelle [TRADUCTION] « [r]ien ne tend à indiquer que Telus était contractuellement tenue de protéger la confidentialité de quelque document que ce soit » militait contre la reconnaissance à l'appelant de la qualité requise pour invoquer l'art. 8 (par. 31). Je reconnais que ce facteur joue contre l'appelant, mais à mon avis seulement jusqu'à un certain point. Lorsqu'on le considère au regard de l'ensemble des circonstances, ce facteur ne fait pas échec à la prétention de l'appelant selon laquelle il a qualité pour agir.

[48] This Court's decisions indicate that because s. 8 "sets out normative limitations on state power . . . its scope cannot . . . be (entirely) dictated

[48] Il ressort de la jurisprudence de notre Cour que, comme l'art. 8 [TRADUCTION] « assortit les pouvoirs de l'État de limitations normatives [. . .],

by exogenous norms like statute or contract" (S. Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014), 67 *S.C.L.R.* (2d) 505, at p. 519).

[49] In *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, Deschamps J. reasoned for the plurality that "the fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative" (para. 34). She also warned that when dealing with contracts of adhesion, in particular, it was necessary to "procee[d] with caution" when determining the impact they may have on one's reasonable expectation of privacy (para. 33). In *Spencer*, Cromwell J. held for a unanimous Court that Mr. Spencer had a reasonable expectation of privacy in the subscriber information notwithstanding that his sister was the subscriber, and hence party to the contract with the service provider (see paras. 7, 12 and 57). Further, he held that to the extent the contract contemplated dissemination of the subscriber information, it provided "little assistance in evaluating the reasonableness of Mr. Spencer's expectation of privacy" (para. 55).

[50] Therefore, in both *Gomboc* and *Spencer*, the *presence* of agreements permitting dissemination of the subject matter of the search could not singularly defeat the claimants' reasonable expectations of privacy.

[51] It follows *a fortiori* that the *absence* of any such agreement here does not defeat Mr. Jones' reasonable expectation of privacy.

sa portée ne saurait [. . .] être (entièrement) définie par des normes exogènes telles des dispositions législatives ou contractuelles » (S. Penney, « The Digitization of Section 8 of the Charter : Reform or Revolution? » (2014), 67 *S.C.L.R.* (2d) 505, p. 519).

[49] Dans l'arrêt *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211, la juge Deschamps a expliqué, au nom d'une pluralité de juges, que « le fait que la personne qui revendique une attente quant au respect du caractère privé de certains renseignements aurait dû savoir que les dispositions régissant ses rapports avec le détenteur de ces renseignements en permettaient la communication n'est pas nécessairement déterminant » (par. 34). La juge Deschamps a également fait la mise en garde suivante, à savoir que, particulièrement dans le cas des contrats d'adhésion, « la prudence est [. . .] de mise » lorsqu'il s'agit de déterminer les conséquences de dispositions de ce genre sur la reconnaissance d'une attente raisonnable au respect de la vie privée (par. 33). Rédigeant l'arrêt unanime de la Cour dans l'arrêt *Spencer*, le juge Cromwell a conclu que M. Spencer avait une attente raisonnable au respect de sa vie privée à l'égard des renseignements relatifs à l'abonné, malgré le fait que l'abonnée était sa sœur et que, en conséquence, c'était elle qui était partie au contrat avec le fournisseur de services (voir par. 7, 12 et 57). Le juge Cromwell a également conclu que, dans la mesure où le contrat envisageait la possibilité de communiquer des renseignements relatifs à l'abonné, les dispositions applicables n'étaient « guère utiles pour évaluer le caractère raisonnable de l'attente de M. Spencer au respect de sa vie privée » (par. 55).

[50] Par conséquent, tant dans l'affaire *Gomboc* que dans l'affaire *Spencer*, la *présence* d'ententes permettant la communication de l'objet de la fouille ou de la perquisition ne pouvait à elle seule écarter l'attente raisonnable des demandeurs au respect de leur vie privée.

[51] A fortiori, il s'ensuit que l'*absence* de pareille entente en l'espèce ne saurait écarter l'attente raisonnable de M. Jones au respect de sa vie privée.

(c) *That the Production Order Targeted a Third Party's Account Does Not Render Mr. Jones' Expectation of Privacy Unreasonable*

[52] The respondent Crown for Ontario argues that the fact that the Production Order targeted a third party's cellphone account rather than Mr. Jones' works against his claim for standing. In my view, it does not. As explained above, a sender of a text message has a reasonable expectation of privacy in that message when it is in the hands of a telecommunications intermediary. In this case, it makes no difference whether the message was accessed through an authorization to peer into the recipient's account or the sender's account. In either case, the Text Messages are in the hands and control of the service provider.

[53] The Ontario Court of Appeal's decision in *R. v. Shayesteh* (1996), 31 O.R. (3d) 161, speaks to this point. In that case, Charron J.A. (as she then was) rejected the Crown's argument that a person who was not targeted by a Part VI authorization had no standing to challenge the authorization. Instead, she held that the applicant's standing was grounded in the fact that his "own telephone calls were intercepted as a result of the targeting" of a third party (p. 173). This was sufficient to "give him standing to dispute the legality" of the impugned interceptions (p. 174).

[54] In the circumstances of this case, the analogy to *Shayesteh* is apt. While the Production Order targeted a third party, it was the appellant's own text message communications that were seized from Telus. As in *Shayesteh*, then, the fact that the authorization targeted a third party, but not Mr. Jones, does not militate against his reasonable expectation of privacy. Holding otherwise would ignore that, pursuant to *PIPEDA*, service providers at large may be expected to maintain privacy over individuals'

c) *Le fait que l'Ordonnance de communication ciblait le compte d'un tiers ne rend pas déraisonnable l'attente de M. Jones au respect de sa vie privée*

[52] La Couronne ontarienne intimée plaide que le fait que l'Ordonnance de communication ciblait un compte de téléphone cellulaire appartenant à un tiers plutôt qu'à M. Jones milite contre la reconnaissance à ce dernier de la qualité pour agir. À mon avis, ce n'est pas le cas. Comme je l'ai expliqué précédemment, l'expéditeur d'un message texte a une attente raisonnable au respect de sa vie privée relativement à ce message lorsqu'il se trouve entre les mains d'un service de télécommunication agissant comme intermédiaire. En l'espèce, le fait que l'accès au message ait été obtenu au moyen d'une autorisation permettant de scruter le compte du destinataire ou celui de l'expéditeur ne change rien à la situation. Dans un cas comme dans l'autre, les Messages textes sont en la possession du fournisseur de services et à sa disposition.

[53] L'arrêt *R. c. Shayesteh* (1996), 31 O.R. (3d) 161, rendu par la Cour d'appel de l'Ontario, porte sur cette question. Dans cette affaire, la juge Charron (plus tard juge de notre Cour) a rejeté l'argument de la Couronne suivant lequel une personne qui n'était pas ciblée par une autorisation visée à la partie VI n'avait pas qualité pour contester cette autorisation. Elle a plutôt conclu que la qualité pour agir du demandeur en cause reposait sur le fait que [TRADUCTION] « ses appels téléphoniques personnels avaient été interceptés par suite d'une autorisation ciblant » un tiers (p. 173). Ce fait était suffisant pour « lui conférer la qualité requise pour attaquer la légalité » des interceptions contestées (p. 174).

[54] Eu égard aux circonstances de l'espèce, l'analogie avec l'affaire *Shayesteh* est appropriée. Même si l'Ordonnance de communication visait un tiers, ce sont les propres messages textes de l'appelant qui ont été saisis chez Telus. En conséquence, tout comme dans *Shayesteh*, le fait que l'autorisation visait un tiers et non M. Jones ne milite pas contre l'attente raisonnable de ce dernier au respect de sa vie privée. Conclure différemment reviendrait à faire abstraction du fait que, sous le régime de la

information, regardless of whether law enforcement targets one disinterested provider over the other.

[55] As a result, I conclude that on the totality of the circumstances, Mr. Jones has a reasonable expectation of privacy in the impugned Text Messages. He accordingly has standing to challenge the validity of the Production Order.

B. *Reasonableness of the Search: Can Historical Text Messages Lawfully Be Seized by Means of a Production Order Under Section 487.014?*

[56] The question remaining is whether, at the second stage of the s. 8 framework, the search and seizure of records of historical text messages pursuant to a production order under what is now s. 487.014 of the *Code* was reasonable. The application judge and the Court of Appeal held that it was. The appellant's argument to the contrary is two-pronged. First, he argues that the courts below erred because the seizure of text messages from the service provider's infrastructure is an "intercept" within the meaning of Part VI of the *Code*. Second, he says that even if the police technique in this case was not, strictly speaking, an "intercept", it was functionally equivalent to one. On either view, it would follow that a Part VI "wiretap" authorization was required to permit the seizure of the Text Messages stored in Telus' infrastructure.

[57] A search "will be reasonable if it is authorized by law, if the law itself is reasonable and if the manner in which the search was carried out is reasonable" (*Collins*, at p. 278). Here, the search

LPRPDE, il est permis de s'attendre à ce que les fournisseurs de services en général protègent le caractère privé des renseignements relatifs à une personne, indépendamment de la question de savoir si les forces de l'ordre visent un fournisseur de services désintéressé plutôt qu'un autre.

[55] Par conséquent, je conclus que, au regard de l'ensemble des circonstances, M. Jones a une attente raisonnable au respect de sa vie privée relativement aux Messages textes en cause et qu'il a de ce fait qualité pour contester la validité de l'Ordonnance de communication.

B. *Caractère non abusif de la fouille : Des messages textes existants peuvent-ils être légalement saisis au moyen d'une ordonnance de communication fondée sur l'art. 487.014?*

[56] La question qui reste à trancher consiste à décider, à la seconde étape du cadre d'analyse de l'art. 8, si la fouille et la saisie des relevés contenant les messages textes existants exécutées en vertu de l'Ordonnance de communication fondée sur la disposition correspondant à l'art. 487.014 actuel du *Code* étaient abusives ou non. Tant la juge saisie de la demande que la Cour d'appel ont conclu que la fouille et la saisie n'étaient pas abusives. La prétention contraire de l'appelant comporte deux volets. Premièrement, il soutient que les juridictions inférieures ont commis une erreur, parce que les messages textes saisis dans l'infrastructure du fournisseur de services ont été « interceptés » au sens de la partie VI du *Code*. Deuxièmement, il affirme que, même si la technique employée par les policiers en l'espèce n'a pas, à strictement parler, consisté à « intercepter » les messages, il s'est agi fonctionnellement d'une mesure équivalente. Dans un cas comme dans l'autre, il s'ensuit selon lui qu'une autorisation de « mise sur écoute électronique » délivrée en vertu de la partie VI était nécessaire afin de pouvoir saisir les Messages textes conservés dans l'infrastructure de Telus.

[57] Une fouille « ne sera pas abusive si elle est autorisée par la loi, si la loi elle-même n'a rien d'abusif et si la fouille n'a pas été effectuée d'une manière abusive » (*Collins*, p. 278). En l'espèce, la

was authorized under s. 487.012 of the *Code* (now s. 487.014) — but the issue is whether this was a proper source of authority for the search in question. Since the parties agree that text messages are private communications protected by Part VI, the question of statutory interpretation this Court must resolve is whether the word "intercept" in s. 183 of the *Code* encompasses the production or seizure of historical text messages held by a service provider. To be clear, the term "historical text messages" denotes text messages that have been sent and received (or are no longer capable of reception), not text messages that are in the *transmission process*. It is only historical text messages — and not those in the transmission process — that are at issue in this appeal.

[58] As the trial judge and the Court of Appeal recognized, *TELUS* did not answer the question at hand. Writing for the plurality, Abella J. limited herself to the issue of whether a Part VI authorization was required for the "*prospective* production of future text messages" (para. 15 (emphasis in original)). Similarly, Moldaver J.'s opinion that the police technique in *TELUS* was substantively equivalent to an intercept was based on the fact it "*prospectively* authorize[d] police access to *future* private communications on a *continual* basis over a sustained period of time" (para. 61 (emphasis in original)). In dissent, Cromwell J. went further and addressed the question at issue here; i.e., whether police could obtain stored text messages by means of a production order (para. 116).

[59] In my view, when the relevant words in ss. 184 and 184(1) are read in "their entire context and in their grammatical and ordinary sense harmoniously" with Part VI's scheme and undergirding purpose, they do not support the appellant's interpretation (*Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at para. 21, quoting E. A. Driedger, *Construction of*

fouille était autorisée sous le régime de l'art. 487.012 (maintenant l'art. 487.014) du *Code*, mais il faut décider si cette disposition constituait la source appropriée pour valider la fouille en question. Étant donné que les parties s'accordent pour dire que les messages textes sont des communications privées protégées par la partie VI, la question d'interprétation législative que doit trancher notre Cour est celle de savoir si le mot « intercepter » à l'art. 183 du *Code* couvre la communication ou la saisie de messages textes existants en possession d'un fournisseur de services. Il convient de préciser que le terme « messages textes existants » s'entend de messages textes qui ont été expédiés et reçus (ou qui ne peuvent plus être reçus), et non pas de messages *en cours de transmission*. Seuls sont en litige dans le présent pourvoi des messages textes existants — et non des messages en cours de transmission.

[58] Comme l'ont reconnu la juge du procès et la Cour d'appel, l'arrêt *TELUS* n'a pas répondu à la question qui se pose en l'espèce. S'exprimant au nom d'une pluralité de juges, la juge Abella a limité son examen à la question de savoir si une autorisation prévue à la partie VI était requise à l'égard de « la communication *prospective* de futurs messages textes » (par. 15 (en italique dans l'original)). De même, l'opinion du juge Moldaver suivant laquelle la technique utilisée par les policiers dans l'affaire *TELUS* équivalait sur le plan du fond à une interception était basée sur le fait qu'elle « permet[tait] *prospectivement* à la police d'accéder à des communications privées *futures* de façon *continue* pendant une période prolongée » (par. 61 (en italique dans l'original)). Dans ses motifs dissidents, le juge Cromwell a poussé l'examen et s'est penché sur la question en litige dans le présent pourvoi, c'est-à-dire celle de savoir si des policiers pouvaient, au moyen d'une ordonnance de communication, obtenir des messages textes conservés (par. 116).

[59] À mon avis, il ressort de la lecture des termes pertinents de l'art. 184 et du par. 184(1), considérés « dans leur contexte global en suivant le sens ordinaire et grammatical qui s'harmonise » avec la structure et l'objectif sous-jacent de la partie VI, que ces termes n'appuient pas l'interprétation proposée par l'appelant (*Rizzo & Rizzo Shoes Ltd. (Re)*,

Statutes (2nd ed. 1983), at p. 87). Nor, in my view, is the police technique in this case an interception within the meaning of s. 184(1) that would require a Part VI authorization. I therefore conclude that police may lawfully obtain the contents of historical text messages by means of a production order under s. 487.014 of the *Code*.

(1) Purpose of Part VI

[60] I turn first to the purpose of Part VI of the *Criminal Code*. Part VI of the *Code* protects individuals' private communications from interception and surveillance by the state. In *R. v. Duarte*, [1990] 1 S.C.R. 30, La Forest J. cast its purpose as follows:

> The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it . . . has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. . . . Rather, the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.
>
> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. [Emphasis added; pp. 43-44.]

Two important observations follow from this passage. The first is that there is distinction between disclosure of information and the interception of private communications through electronic surveillance. The second is that, as La Forest J. explained, Part VI is particularly concerned with regulating the use of intrusive investigation technologies and their impact on citizens' privacy, not the protection of private communications at large. As explained below,

[1998] 1 R.C.S. 27, par. 21, citant E. A. Driedger, *Construction of Statutes* (2e éd. 1983), p. 87). Je ne considère pas non plus que la technique policière utilisée en l'espèce constitue une interception visée au par. 184(1) qui exigerait une autorisation fondée sur la partie VI. Je conclus donc que les policiers peuvent légalement obtenir le contenu de messages textes existants au moyen d'une ordonnance de communication prévue à l'art. 487.014 du *Code*.

(1) L'objet de la partie VI

[60] Je vais d'abord examiner l'objet de la partie VI du *Code criminel*. Cette partie protège les communications privées des particuliers contre les activités de surveillance et d'interception de l'État. Dans l'arrêt *R. c. Duarte*, [1990] 1 R.C.S. 30, le juge La Forest a défini ainsi l'objet de la partie VI :

> La raison d'être de la réglementation du pouvoir de l'État d'enregistrer des communications dont l'auteur s'attend à ce qu'elles ne soient entendues que par leur destinataire [. . .] n'a rien à voir avec la protection de particuliers contre la menace que leurs interlocuteurs divulguent des communications censément privées. [. . .] La réglementation de la surveillance électronique nous protège plutôt contre un risque différent : non plus le risque que quelqu'un répète nos propos, mais le danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos.
>
> Cette protection s'explique par la conscience du fait que, si l'État était libre de faire, à son entière discrétion, des enregistrements électroniques permanents de nos communications privées, il ne nous resterait rien qui vaille de notre droit de vivre libre de toute surveillance. La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications restent privées. [Je souligne; p. 43-44.]

Deux observations importantes découlent des passages précités. En premier lieu, il convient de distinguer entre, d'une part, la divulgation de renseignements et, d'autre part, l'interception de communications privées par voie de surveillance électronique. En second lieu, comme l'a expliqué le juge La Forest, la partie VI vise particulièrement à régir l'utilisation de techniques d'enquête envahissantes et l'incidence de celles-ci sur la vie privée des

both of these aspects of Part VI's purpose should be borne in mind in resolving the issue at hand.

(2) The Structure of Part VI and the Distinction Between Interception and Disclosure

[61] As the Court of Appeal recognized, Part VI's structure reflects the distinction between interception and disclosure. Sections 184 to 192 offer protection against the interception of private communications. Section 193 prohibits the disclosure of information obtained through intercepted communications. This dual structure reflects Parliament's purpose because it created distinct offences for interception and disclosure.

[62] The first of these offences, set out in s. 184 of the *Code*, prohibits the interception of private communications by the use of certain devices unless one of the legislated exemptions in s. 184(2) applies. Under s. 182(2)(e), telecommunication service providers like Telus are exempted from the interception offence if they intercept communications for service delivery reasons. Section 184(3) then specifically addresses the *use* or *retention* of previously intercepted communications. It provides that:

Use or retention

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

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

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

[63] What is significant is that this section of the scheme clearly distinguishes "between *interception* on the one hand and *use* or *retention* of the intercepted communications on the other" (*TELUS*, at

citoyens, et non à encadrer la protection des communications privées au sens large. Ainsi que je vais l'expliquer, il convient de garder à l'esprit ces deux aspects de l'objet de la partie VI afin de trancher la question en litige.

(2) La structure de la partie VI et la distinction entre interception et divulgation

[61] Comme l'a reconnu la Cour d'appel, la structure de la partie VI reflète la distinction qui existe entre l'interception et la divulgation. Les articles 184 à 192 établissent des mesures de protection contre l'interception des communications privées. L'article 193 prohibe la divulgation de renseignements obtenus au moyen des communications interceptées. Cette dualité structurale traduit l'objectif visé par le législateur, en ce que ce dernier a créé des infractions distinctes pour l'acte d'interception et l'acte de divulgation.

[62] La première de ces infractions, énoncée à l'art. 184 du *Code*, interdit l'interception des communications privées au moyen de certains dispositifs, sauf si l'une des exceptions légales prévues au par. 184(2) s'applique. Suivant l'al. 182(2)e), les fournisseurs de services de télécommunication comme Telus jouissent d'une immunité à l'égard de l'infraction d'interception s'ils interceptent des communications dans le cadre de la fourniture de leurs services. Le paragraphe 184(3) traite expressément de l'*utilisation* ou *conservation* de communications déjà interceptées. Voici le texte de cette disposition :

Utilisation ou conservation

(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).

[63] L'élément important est le fait que cette disposition du régime distingue nettement « *l'interception* de la communication, d'une part, de *l'utilisation* ou de *la conservation* de la communication interceptée,

para. 143, per Cromwell J. (emphasis in original)). "This suggests that Parliament viewed those acts as different and distinct" (*ibid.*, at para. 144).

[64] Section 193 is concerned with disclosure:

Disclosure of information

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.

[65] Section 193 makes it an offence to *disclose* a private communication that *has been intercepted*, subject to the exceptions in s. 193(2). Under these exceptions, disclosure is not an offence where, *inter alia*, the disclosure of a previously intercepted communication is made "in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted" (s. 193(2)(b)), or when disclosure is made to a police officer and is "intended to be in the interests of the administration of justice in Canada" (s. 193(2)(e)).

[66] In this case, there is no question that Telus initially intercepted the communications between Mr. Jones and Mr. Waldron, presumably pursuant to an exception under s. 184(2) of the *Code*. However, in light of the statutory scheme's explicit distinction between *interception, use and retention*, and *disclosure*, it is clear that Telus' subsequent storing and provision of the communications to the law

d'autre part » (*TELUS*, par. 143, le juge Cromwell (en italique dans l'original)), « ce qui indique que le législateur y voyait des actes différents et distincts » (*ibid.*, par. 144).

[64] L'article 193 porte sur la divulgation :

Divulgation de renseignements

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.

[65] Aux termes de l'art. 193, constitue une infraction le fait pour quiconque de *divulguer* une communication privée qui *a été interceptée*, sous réserve des exceptions prévues au par. 193(2). Suivant ces exceptions, la divulgation ne constitue pas une infraction lorsque, par exemple, la divulgation d'une communication déjà interceptée survient « au cours ou aux fins d'une enquête en matière pénale, si la communication privée a été interceptée légalement » (al. 193(2)b)), ou lorsque la divulgation est faite à un agent de la paix et « vise à servir l'administration de la justice au Canada » (al. 193(2)e)).

[66] Dans le cas qui nous occupe, il ne fait aucun doute que les communications échangées entre MM. Jones et Waldron ont initialement été interceptées par Telus en vertu, vraisemblablement, d'une des exceptions prévues au par. 184(2) du *Code*. Toutefois, compte tenu de la distinction explicite que le régime législatif établit entre l'*interception*, l'*utilisation* et la *conservation* d'une part, ainsi que la

enforcement did not constitute additional *interceptions*. Rather, to use the language in Part VI, Telus *retained* the intercepted communications under s. 184(3) and then *disclosed* them to the police as contemplated by s. 193(2). The appellant's tendered interpretation is difficult to reconcile with these distinctions made within Part VI.

(3) The Plain Meaning of "Intercept" and Its Surrounding Context

[67] The appellant's tendered interpretation withers further when the word "intercept" is given its plain meaning and read in light of its surrounding context. The crucial context here lies in s. 184(1) and the definition of intercept in s. 183.

[68] Section 184(1) provides that:

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

Intercept is defined in s. 183 as follows:

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

[69] Based on its plain meaning, interception suggests a prospective concept of authorization relating to communications not yet in existence. The word "intercept" denotes an interference between the sender and recipient in the course of the communication process (see *R. v. Belcourt*, 2015 BCCA 126, 322 C.C.C. (3d) 93, at paras. 45-46; *R. v. McQueen* (1975), 25 C.C.C. (2d) 262 (Alta. S.C. (App. Div.)), at p. 265; *R. v. Giles*, 2007 BCSC 1147, at para. 37 (CanLII)). As explained in *TELUS*, the "word 'intercept' implies that the private communication is acquired in the course of the communication

divulgation d'autre part, il est évident que la conservation des télécommunications par Telus et leur divulgation ultérieure par cette dernière aux policiers n'ont pas constitué des *interceptions* additionnelles. Suivant les termes utilisés à la partie VI, Telus a plutôt *conservé* les communications interceptées en vertu du par. 184(3), puis les a ensuite *divulguées* aux policiers comme le prévoit le par. 193(2). Il est difficile de concilier l'interprétation proposée par l'appelant avec les distinctions que fait le législateur à la partie VI.

(3) Le sens courant du mot « intercepter » et son contexte

[67] L'interprétation proposée par l'appelant s'étiole encore davantage lorsqu'on donne au mot « intercepter » son sens courant et qu'on l'interprète à la lumière de son contexte. En l'espèce, les éléments cruciaux du contexte se trouvent au par. 184(1) et dans la définition d'« intercepter » à l'art. 183.

[68] Le paragraphe 184(1) prévoit ce qui suit :

> **(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.

Le mot « intercepter » est défini ainsi à l'art. 183 :

> ***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.

[69] Selon son sens courant, la notion d'interception suggère l'idée d'une autorisation prospective visant des communications qui n'existent pas encore. Le verbe « intercepter » évoque une interposition entre l'expéditeur et le destinataire dans le cours du processus de communication (voir *R. c. Belcourt*, 2015 BCCA 126, 322 C.C.C. (3d) 93, par. 45-46; *R. c. McQueen* (1975), 25 C.C.C. (2d) 262 (C.S. Alb. (Div. app.)), p. 265; *R. c. Giles*, 2007 BCSC 1147, par. 37 (CanLII)). Comme il a été expliqué dans *TELUS*, le « mot "intercepter" implique que la prise de connaissance de la communication

process" (para. 37). It follows that in order for a Part VI authorization to permit a real-time intercept of the communication, it must be granted in advance of that communication. That is, it must be *prospective*. As the Court of Appeal for Ontario recently observed, "[t]he words sought for capture do not exist when the [Part VI] authorization is granted. They may never exist or disclose anything of relevance to any offence under investigation" (*R. v. Beauchamp*, 2015 ONCA 260, 326 C.C.C. (3d) 280, at para. 93).

privée se fait au cours du processus de transmission » (par. 37). Il s'ensuit que, pour qu'une autorisation visée à la partie VI permette l'interception d'une communication en temps réel, elle doit avoir été accordée préalablement à cette communication. Autrement dit, elle doit avoir un effet *prospectif*. Comme l'a récemment fait observer la Cour d'appel de l'Ontario, [TRADUCTION] « [l]es propos que l'on souhaite saisir n'existent pas encore lorsque l'autorisation [visée à la partie VI] est accordée. Il est possible qu'ils ne se matérialisent jamais ou qu'ils ne révèlent rien de pertinent en ce qui concerne l'infraction faisant l'objet de l'enquête » (*R. c. Beauchamp*, 2015 ONCA 260, 326 C.C.C. (3d) 280, par. 93).

[70] While the definition of "intercept" in s. 183 of the *Code* may read broadly because it features the word "acquire", a comparison with the French version of the provision reinforces the conclusion that Part VI authorizations relate only to future communications. As the intervener the Director of Criminal and Penal Prosecutions points out, the French version diverges from the English by employing the words "*prendre . . . connaissance*" in lieu of "acquire". This is contrasted with numerous other sections of the *Code* where Parliament translated the English "acquire" to the French "*obtenir*" or "*acquérir*" (see, e.g., ss. 164.2(1)(b)(ii), 164.3(4)(b), 462.34(6)(a)(ii), 462.41(3)(b), 462.42(1)(b), 490.4(3) and 490.5(1)(c)). The distinct translation here suggests a different meaning than in those other contexts.

[70] Bien que la définition du mot « intercepter » à l'art. 183 du *Code* puisse se prêter à une interprétation large vu la présence du mot « *acquire* » dans la version anglaise, la comparaison des versions anglaise et française de la définition renforce la conclusion que l'autorisation visée à la partie VI ne vise que des communications futures. Comme le souligne un des intervenants, le directeur des poursuites criminelles et pénales, le texte français diverge du texte anglais du fait qu'on y utilise le terme « prendre [. . .] connaissance » comme équivalent du mot anglais « *acquire* ». Cette formulation contraste avec celle de nombreux autres articles du *Code* où le législateur a fait correspondre au terme anglais « *acquire* » les mots « obtenir » ou « acquérir », selon le cas, en français (voir, p. ex., le sous-al. 164.2(1)b)(ii), l'al. 164.3(4)b), le sous-al. 462.34(6)a)(ii), les par. 462.41(3), 462.42(1) et 490.4(3) et l'al. 490.5(1)c)). Le terme distinct utilisé à l'art. 183 tend à indiquer un sens différent de celui exprimé dans ces autres contextes.

[71] Further, the word "acquire" in s. 183 must be read alongside the words surrounding it. As Justice Cromwell observed in *TELUS*:

[71] De plus, le mot « *acquire* » utilisé dans la version anglaise de l'art. 183 doit être interprété en corrélation avec les mots qui l'entourent. Comme l'a fait remarquer le juge Cromwell dans l'arrêt *TELUS* :

. . . "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

. . . 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

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. [para. 155]

[72] Finally, the definition of intercept in s. 183 must be understood in the context of s. 184, which is at the heart of Part VI and makes it an offence to intercept communications "by means of any electromagnetic, acoustic, mechanical or other device". For example, past practice has been that where police obtain a Part VI authorization to intercept future text messages, "Telus installs a device which automatically re-routes a copy of each text message to a police wire room or listening post" (*TELUS*, at para. 122). This clarifies that interception relates to actions by which a third party interjects itself into the communication process in real-time through technological means.

[73] This understanding of "intercept" coheres with Part VI's overall purpose. Recall that the policy motivating Part VI was a concern with the use of intrusive surveillance technologies and their impact on citizens' privacy (*Duarte*, at pp. 43-44). State surveillance may be continuous over a prolonged period of time and gives the police real-time access to information they would otherwise have to wait for, putting them in a better position to "conduct physical surveillance and gather physical evidence that might not be available later" (I.F. (Attorney General of British Columbia), at para. 31).

[74] Added to these concerns is the fear that when equipped with sophisticated surveillance technologies, the state may be tempted to embark on forward-looking, "fishing expedition[s] in the hope of uncovering evidence of crime" (*R.*

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. [par. 155]

[72] Enfin, la définition du mot intercepter à l'art. 183 doit être interprétée en fonction du contexte de l'art. 184, disposition qui est au cœur de la partie VI et qui érige en infraction le fait d'intercepter des communications « au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre ». Par exemple, suivant la pratique suivie jusqu'ici, lorsque les policiers obtiennent en vertu de la partie VI une autorisation leur permettant d'intercepter des messages textes futurs, « Telus installe un dispositif qui achemine automatiquement une copie de chaque message texte à la salle ou au poste d'écoute de la police » (*TELUS*, par. 122). Ces clarifications permettent de comprendre que l'interception correspond aux actes accomplis par un tiers qui s'interpose en temps réel dans le processus de communication en recourant à des moyens technologiques.

[73] Cette façon de comprendre le mot « intercepter » s'accorde avec l'objectif général de la partie VI. Il convient de rappeler que l'adoption de la partie VI était motivée par les inquiétudes que soulevaient l'utilisation de moyens technologiques de surveillance envahissants ainsi que l'incidence de ceux-ci sur la vie privée des citoyens (*Duarte*, p. 43-44). Les mesures de surveillance utilisées par l'État peuvent se dérouler de façon continue pendant de longues périodes. En outre, elles permettent aux policiers d'avoir accès en temps réel à des renseignements à l'égard desquels ils auraient autrement à attendre, ce qui les place dans une meilleure situation pour [TRADUCTION] « exercer une surveillance physique et recueillir des éléments de preuve matériels qui pourraient ne plus exister ultérieurement » (m.i. (procureur général de la Colombie-Britannique), par. 31).

[74] Outre ces inquiétudes, mentionnons la crainte que, muni de moyens technologiques avancés de surveillance, l'État soit tenté de se livrer à des [TRADUCTION] « recherche[s] à l'aveuglette [prospectives] dans l'espoir de découvrir des indices d'un

v. Finlay (1985), 23 C.C.C. (3d) 48 (Ont. C.A.), at p. 70; see also *Belcourt*, at para. 47). It is that potential temptation which requires us to be "alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy" (*Wong*, at p. 47). The constitutionality of the interception scheme accordingly stems from the heightened safeguards Part VI imposes in light of the dangers created by prospective authorizations (*Belcourt*, at para. 47; *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 29). As a result of these safeguards, "[a]n application for a conventional authorization to intercept private communications is" — in the words of one commentator — "the most exacting pre-trial investigative proceeding known to our criminal law" (S. C. Hutchison et al., *Search and Seizure Law in Canada* (loose-leaf), vol. 1, at p. 4-37 (footnote omitted)). Based on the statutory scheme, the disclosure of previously stored records does not trigger these concerns, and is accordingly not subject to these safeguards.

crime » (*R. c. Finlay* (1985), 23 C.C.C. (3d) 48 (C.A. Ont.), p. 70; voir également *Belcourt*, par. 47). C'est cette tentation potentielle qui nous oblige à « rester conscient[s] du fait que les moyens modernes de surveillance électronique, s'ils ne sont pas contrôlés, sont susceptibles de supprimer toute vie privée » (*Wong*, p. 47). La constitutionnalité du régime d'interception résulte en conséquence des garanties accrues dont la partie VI impose le respect pour tenir compte des dangers que créent les autorisations prospectives (*Belcourt*, par. 47; *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992, par. 29). En raison de ces garanties, [TRADUCTION] « [u]ne demande visant à obtenir une autorisation traditionnelle d'interception de communications privées est » — pour reprendre la formule d'un commentateur — « la procédure d'enquête préalable au procès la plus exigeante qui existe dans notre droit criminel » (S. C. Hutchison et autres, *Search and Seizure Law in Canada* (feuilles mobiles), vol. 1, p. 4-37 (note en bas de page omise)). Compte tenu du régime établi par la loi, la divulgation de relevés déjà conservés ne suscite pas de telles inquiétudes et n'est donc pas assujettie au respect de ces garanties.

(4) The Police Technique Engaged in This Case Is Not an Interception

[75] Unlike the police technique in *TELUS*, the technique in this case does not bear the hallmarks of an interception. In *TELUS*, the police sought a *prospective* order securing the recording and preservation of *future* messages, along with their automatic and continuous disclosure to police each day for a two-week period (para. 42). This made the investigative technique "substantively equivalent to an intercept" (para. 52 (emphasis deleted)). The police in *TELUS* effectively deputized the service provider by requiring it to provide them with daily and comprehensive briefings of the targeted parties' communications.

[76] In contrast, the Production Order in this case, dated February 12, 2010, sought text messaging information and records relating to a prior

(4) La technique policière utilisée en l'espèce ne constitue pas une interception

[75] Contrairement à la technique policière en cause dans l'affaire *TELUS*, celle employée en l'espèce ne présente pas les caractéristiques d'une interception. Dans *TELUS*, les policiers avaient sollicité une ordonnance *prospective* afin d'obtenir l'enregistrement et la conservation de messages *futurs*, en plus de leur divulgation systématique et continue sur une base quotidienne pendant une période de deux semaines (par. 42). Cette caractéristique rendait la technique d'enquête « équivalente, sur le plan du fond, à une interception » (par. 52 (italique omis)). Les policiers avaient, dans cette affaire, concrètement fait du fournisseur de services leur adjoint en exigeant de celui-ci qu'il leur transmette chaque jour un compte rendu détaillé des communications échangées entre les parties ciblées.

[76] Par comparaison, dans le cas qui nous occupe, l'Ordonnance de communication datée du 12 février 2010 visait des messages textes et de l'information

period beginning January 5, 2010 and ending February 12, 2010. Although the Order requests text messages sent or received on the date of the authorization itself, there is no evidence to the effect that some of the texts produced by Telus were in the transmission process on February 12, 2010 at the time the Order was made. In the absence of such evidence, and in light of the fact that Telus was given 30 days to comply with the Order, it would be speculative to infer that the Order operated *prospectively* so as to catch *future* text messages. Nor is there any evidence that the messages were stored and retained as part of Telus' communicative process. Nor still is there evidence that Telus stored the messages at the request of the police or for law enforcement purposes. Finally, subsequent to the Production Order, when the police sought to intercept *future* communications between Mr. Jones and Mr. Waldron, they properly requested and obtained two Part VI authorizations dated November 12, 2010 and January 12, 2011, respectively.

s'y rapportant pour la période du 5 janvier 2010 au 12 février 2010 inclusivement. Quoique l'Ordonnance requière la production des messages textes envoyés ou reçus le jour même de sa délivrance, il n'y a aucune preuve indiquant que certains des messages textes produits par Telus se trouvaient dans le processus de transmission le 12 février 2010, au moment où l'Ordonnance a été rendue. En l'absence de preuve à cet effet, et compte tenu du fait que Telus s'est vu accorder 30 jours pour se conformer à l'Ordonnance, inférer que celle-ci avait un effet *prospectif* et permettait ainsi la saisie de messages textes *futurs* relèverait de la conjecture. Il n'existe pas non plus de preuve que les messages étaient conservés par Telus dans le cadre du processus de communication. Et il n'y a en outre aucun élément de preuve indiquant que Telus avait conservé les messages à la demande des policiers ou aux fins d'application de la loi. Enfin, postérieurement à la délivrance de l'Ordonnance de communication, lorsque les policiers ont souhaité intercepter les communications *futures* entre MM. Jones et Waldron, ils ont, comme ils se devaient de le faire, demandé et obtenu en vertu de la partie VI deux autorisations datées respectivement du 12 novembre 2010 et du 12 janvier 2011.

[77] In short, the state action in this case respected Part VI's distinction between the interception of communications in ss. 184 to 192 and the disclosure of previously intercepted and stored communications as contemplated by s. 193. Based on the evidence, it also respected the requirement in *TELUS* that a Part VI authorization be obtained for text messages that are still in the transmission process. Law enforcement cannot receive authorization to effectively intercept future communications through the "backdoor" of the general search and seizure regime in s. 487 of the *Code*. But law enforcement could — and did, in this case — lawfully obtain records of historical text messages by means of a Production Order under s. 487.012 of the *Code* (as they can still do now under s. 487.014).

[77] En résumé, les mesures prises par l'État en l'espèce respectaient la distinction établie à la partie VI entre l'interception des communications aux art. 184 à 192, et la divulgation de communications déjà interceptées et conservées qui est envisagée à l'art. 193. À la lumière de la preuve, ces mesures respectaient également l'exigence établie dans l'arrêt *TELUS* et suivant laquelle une autorisation fondée sur la partie VI doit être obtenue à l'égard de messages qui se trouvent toujours dans le processus de transmission. Les personnes chargées de l'application de la loi ne peuvent se voir accorder, par le « moyen détourné » que constituerait le régime général prévu à l'art. 487 du *Code* en matière de fouilles, perquisitions et saisies, l'autorisation d'intercepter concrètement des communications futures. Elles pouvaient toutefois — et ce fut le cas en l'espèce — obtenir légalement des copies de messages textes existants au moyen d'une ordonnance de communication fondée sur l'art. 487.012 du *Code* (comme elles peuvent encore le faire en vertu maintenant de l'art. 487.014).

[78] I am mindful of the fact that text messages are inherently private and in many ways akin to conversations. However, the need for a Part VI authorization does not vary with the level of privacy engaged by a state search. For example, as Justice Fish observed in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, it is "difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer" (para. 2). And indeed, like phones or service providers, computers may contain stored records of digital conversations. Yet this Court has always held that seizures of computers may be authorized under the general regime in s. 487 of the *Code* (*R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *Cole*; *Morelli*). As the Court of Appeal recognized, whether or not a Part VI authorization is required "comes down to the specific investigative technique used by the police, and whether that technique constitutes an interception of private communications" (para. 32).

[78] Je suis consciente du fait que les messages textes ont un caractère intrinsèquement privé et qu'ils sont sous de nombreux rapports assimilables à des conversations. Toutefois, la nécessité d'obtenir une autorisation en vertu de la partie VI ne varie pas en fonction du degré d'atteinte au droit à la vie privée qu'implique la fouille ou perquisition envisagée par l'État. Par exemple, comme l'a fait observer le juge Fish dans *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, il est « difficile d'imaginer une perquisition, une fouille et une saisie plus envahissantes, d'une plus grande ampleur ou plus attentatoires à la vie privée que celles d'un ordinateur personnel » (par. 2). D'ailleurs, les ordinateurs — tout comme les téléphones et les serveurs et autres dispositifs des fournisseurs de services — peuvent contenir des copies de conversations numériques. Malgré cela, notre Cour a toujours jugé que la saisie d'un ordinateur peut être autorisée en vertu du régime général prévu à l'art. 487 du *Code* (*R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657; *Cole*; *Morelli*). Ainsi que l'a reconnu la Cour d'appel, la question de savoir si l'obtention d'une autorisation visée à la partie VI est nécessaire [TRADUCTION] « dépend en définitive de la technique d'enquête particulière utilisée par les policiers et de la question de savoir si cette technique constitue une interception de communications privées » (par. 32).

[79] It follows that in considering whether or not to grant a production order under s. 487.014(1), the judicial officer seized of the application should reject it where the technique constitutes an interception under s. 184(1). This is evident from the interplay between the wiretap provisions in Part VI and the production order requirements of s. 487.014. With respect to the wiretap provisions, s. 184(2) creates an exemption from the general prohibition in s. 184(1). This provision exempts, in relevant part, interceptions obtained "with an authorization" (s. 184(2)(b)). "Authorization" is a defined term: it "means an authorization . . . given under section 186 or subsection 184.2(3), 184.3(6) or 188(2)" (s. 183). A production order issued under s. 487.014 is *not* an "authorization" for the purposes of Part VI — thus, a production order would not make an interception lawful. With respect to the requirements for a production order, s. 487.014(1) provides that on an "*ex parte*

[79] Il s'ensuit que le juge ou juge de paix saisi d'une demande d'ordonnance de communication fondée sur le par. 487.014(1) devrait la rejeter lorsque la technique employée constitue une interception visée au par. 184(1). C'est ce qui ressort de l'interaction entre les dispositions sur l'écoute électronique de la partie VI et les exigences relatives à l'ordonnance de communication de l'art. 487.014. En ce qui a trait aux dispositions sur l'écoute électronique, le par. 184(2) énonce une exception à l'interdiction générale prévue au par. 184(1). Selon cette disposition, les interceptions obtenues « en conformité avec une autorisation » (al. 184(2)b)) ne sont pas assujetties à cette interdiction. Le terme « autorisation » est défini ainsi à l'art. 183 : « Autorisation d'intercepter une communication privée donnée en vertu de l'article 186 ou des paragraphes 184.2(3), 184.3(6) ou 188(2). » Une ordonnance de communication rendue conformément à l'art. 487.014 *n'*est

application made by a peace officer or public officer, a justice or judge may order a person to produce a document". The *Code* therefore confers a discretion on the justice or judge to be exercised in accordance with the conditions set out in s. 487.014(2). In exercising this discretion, the judicial officer should consider whether or not the technique sought to be authorized under the auspices of s. 487.014 is an intercept within the meaning of s. 184(1). Where it is, a production order should be denied because the interception would nevertheless be unlawful absent a Part VI authorization.

[80] Production orders must therefore be carefully circumscribed to ensure that authorized police techniques comply with s. 184(1). A production order must not authorize, or potentially authorize, the production of any text messages that are either not yet in existence or are still capable of delivery at the time the order is issued. This should be clear from the face of the order. Where the technique at issue is an intercept within the meaning of s. 184(1), then the application is properly rejected and a Part VI authorization must be obtained. A production order should not be used to sidestep the more stringent Part VI authorization requirements.

[81] In this case, however, a Part VI authorization was unnecessary because the police did not seek an order authorizing the *prospective* production of *future* text messages. Nor is there any evidence before this Court that the Production Order resulted in the production of text messages that were still in the transmission process. Accordingly, the search and seizure of Mr. Jones' text messages were properly authorized by the production order provision

pas une « autorisation » pour l'application de la partie VI — par conséquent, une telle ordonnance ne rendrait pas l'interception légale. Pour ce qui est des exigences relatives à l'ordonnance de communication, le par. 487.014(1) précise que « le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute personne de communiquer un document ». Le *Code* confère donc aux juges et juges de paix un pouvoir discrétionnaire qu'ils doivent exercer conformément aux conditions énumérées au par. 487.014(2). Dans l'exercice de ce pouvoir discrétionnaire, ils doivent se demander si la technique faisant l'objet de la demande d'autorisation présentée en vertu de l'art. 487.014 constitue une interception visée au par. 184(1). Dans l'affirmative, l'ordonnance de communication sollicitée devrait être refusée, car l'interception demeurerait illégale en l'absence d'une autorisation fondée sur la partie VI.

[80] Les ordonnances de communication doivent en conséquence être soigneusement circonscrites afin de garantir que les techniques policières autorisées respectent le par. 184(1). Une ordonnance de communication ne doit pas autoriser concrètement, ni potentiellement, la communication de tout message texte qui n'existe pas encore ou dont la transmission est encore possible au moment où l'ordonnance est délivrée. Cela devrait ressortir clairement du texte même de l'ordonnance. Lorsque la technique en cause constitue une interception visée au par. 184(1), la demande doit à juste titre être rejetée et une autorisation visée à la partie VI doit être obtenue. Une ordonnance de communication ne devrait pas être utilisée pour éluder les exigences plus sévères qui s'appliquent à l'égard des autorisations fondées sur la partie VI.

[81] Toutefois, dans le cas qui nous occupe, il n'était pas nécessaire d'obtenir l'autorisation prévue à la partie VI, étant donné que les policiers ne sollicitaient pas une ordonnance les autorisant à obtenir la communication *prospective* de messages textes *futurs*. Il n'a pas non plus été présenté à la Cour d'éléments de preuve montrant que l'Ordonnance de communication avait entraîné la communication de messages textes qui se trouvaient encore dans le

in s. 487.012 of the *Code* (now s. 487.014), and did not breach Mr. Jones' s. 8 *Charter* right.

III. Conclusion

[82] For these reasons, I would dismiss the appeal and uphold the validity of the Production Order.

The following are the reasons delivered by

[83] ROWE J. — I agree with Justice Côté that, as a matter of statutory interpretation, a production order pursuant to s. 487.014 of the *Criminal Code*, R.S.C. 1985, c. C-46 (pursuant to s. 487.012 in this case), authorizes the police to request the disclosure of text messages from a service provider once those messages have been sent and received. Conversely, a Part VI authorization is required to intercept those messages as they are being transmitted. My comments that follow are *obiter dicta*; they address an issue not dealt with in the judgment, nor raised in argument.

[84] An example is useful. At 8:00 a.m., police obtain an authorization pursuant to Part VI to intercept text messages as they are sent from A to B. Text messages sent from A to B at 9:00 a.m. are intercepted pursuant to this authorization. Alternatively, police at 10:00 a.m. obtain a production order pursuant to s. 487.014 for text messages sent by A to B at 9:00 a.m. In both instances, the police obtain the same information — the text messages sent at 9:00 a.m. The police, however, must meet markedly different requirements depending on which method they choose, with those under Part VI being far more stringent than those under s. 487.014. This seems to me to be highly anomalous.

processus de transmission. Par conséquent, la fouille et la saisie des messages textes de M. Jones ont été régulièrement autorisées en vertu des dispositions relatives aux ordonnances de communication prévues à l'art. 487.012 du *Code* (maintenant l'art. 487.014), et ces mesures n'ont pas porté atteinte aux droits garantis à M. Jones par l'art. 8 de la *Charte*.

III. Dispositif

[82] Pour ces motifs, je rejetterais le pourvoi et je confirmerais la validité de l'Ordonnance de communication.

Version française des motifs rendus par

[83] LE JUGE ROWE — Je suis d'accord avec la juge Côté pour dire que, suivant les règles d'interprétation des lois, l'ordonnance de communication prévue à l'art. 487.014 du *Code criminel*, L.R.C. 1985, c. C-46 (l'art. 487.012 en l'espèce), autorise les policiers à demander à un fournisseur de services de divulguer des messages textes après que ceux-ci ont été envoyés et reçus. En revanche, une autorisation fondée sur la partie VI est requise pour intercepter ces messages pendant leur transmission. Les commentaires qui suivent constituent des remarques incidentes; ils portent sur une question qui n'est pas examinée dans les motifs du jugement, et qui n'a pas non plus été soulevée lors des débats.

[84] Il est utile de donner un exemple. À 8 h, les policiers obtiennent, en vertu de la partie VI, l'autorisation d'intercepter des messages textes au fur et à mesure qu'ils sont envoyés de A à B. Des messages textes envoyés de A à B à 9 h sont interceptés par les policiers en vertu de cette autorisation. Suivant un autre scénario, les policiers obtiennent, à 10 h, une ordonnance de communication prévue à l'art. 487.014 à l'égard des messages textes envoyés de A à B à 9 h. Dans les deux cas, les policiers obtiennent les mêmes renseignements, soit les messages textes envoyés à 9 h. Cependant, ils doivent respecter des exigences nettement différentes selon la méthode qu'ils choisissent d'utiliser, les exigences de la partie VI étant beaucoup plus rigoureuses que celles de l'art. 487.014. Cette situation m'apparaît très anormale.

[85] Are the requirements for a production order under s. 487.014 sufficient to give proper effect to the protection against unreasonable search or seizure under s. 8 of the *Canadian Charter of Rights and Freedoms*? Justice Côté writes that "[a] production order should not be used to sidestep the more stringent Part VI authorization requirements" (para. 80). Given that the records of text messages are stored by Telus the moment they are sent, however, it makes little difference whether the police "intercept" them or simply obtain them through a production order immediately after they are sent. It appears, in other words, that the police can *in effect* sidestep the requirements of Part VI by obtaining a production order immediately after the messages are sent.

[85] Est-ce que les exigences relatives à l'ordonnance de communication prévue à l'art. 487.014 sont suffisantes pour que la protection contre les fouilles, perquisitions et saisies abusives garantie par l'art. 8 de la *Charte canadienne des droits et libertés* produise l'effet voulu? La juge Côté écrit, au par. 80, qu'« [u]ne ordonnance de communication ne devrait pas être utilisée pour éluder les exigences plus sévères qui s'appliquent à l'égard des autorisations fondées sur la partie VI ». Cependant, comme Telus conserve des copies des messages textes dès qu'ils sont envoyés, il importe peu que les policiers les « interceptent » ou les obtiennent tout simplement au moyen d'une ordonnance de communication immédiatement après leur envoi. En d'autres mots, il semble que les policiers peuvent *effectivement* éluder les exigences de la partie VI en obtenant une ordonnance de communication immédiatement après l'envoi des messages.

[86] This sidestepping is only possible because Telus retains records of its customers' text messages. When a Telus customer sends a text message, that message can be obtained via a production order *only* because Telus, as part of its transmission process, keeps a record of all messages sent by their customers. As other major service providers do not at present keep records of their customers' messages, the police would have to obtain a Part VI authorization if they wanted to obtain text messages from Bell or Rogers, for example.

[86] Cette façon de faire est possible uniquement parce que Telus conserve des copies des messages textes de ses clients. Lorsqu'un client de Telus envoie un message texte, ce message peut être obtenu au moyen d'une ordonnance de communication *uniquement* parce que, dans le cadre de son processus de transmission, Telus conserve des copies de tous les messages envoyés par ses clients. Comme les autres grands fournisseurs de services ne conservent pas pour l'instant de copies des messages de leurs clients, les policiers seraient tenus d'obtenir une autorisation fondée sur la partie VI s'ils souhaitaient se procurer des messages textes auprès de Bell ou de Rogers par exemple.

[87] I express no settled view on whether these anomalies reflect the failure of s. 487.014 to meet the requirements imposed by s. 8 of the *Charter*. In the result, I concur with Justice Côté.

[87] Je n'exprime pas d'opinion définitive sur la question de savoir si ces anomalies indiquent que l'art. 487.014 ne respecte pas les exigences de l'art. 8 de la *Charte*. En dernière analyse, je souscris aux motifs exposés par la juge Côté.

The following are the reasons delivered by

Version française des motifs rendus par

[88] Abella J. (dissenting) — The police obtained copies of historical text messages through a Production Order pursuant to s. 487.012 of the

[88] La juge Abella (dissidente) — Les policiers ont obtenu des copies de messages textes existants grâce à une ordonnance de communication

Criminal Code, R.S.C. 1985, c. C-46.[3] Tristin Jones sent these messages to the Telus cellphone account associated with his co-accused. These messages formed the basis of Mr. Jones' conviction for offering to transfer a firearm.

[89] As in the companion case of *R. v. Marakah*, [2017] 2 S.C.R. 608, the first issue is whether the sender of a text message has a reasonable expectation of privacy in copies of his or her sent text messages, and, as a result, standing under s. 8 of the *Canadian Charter of Rights and Freedoms*. Section 8 states:

Everyone has the right to be secure against unreasonable search or seizure.

[90] I agree with Justice Côté that Mr. Jones had a reasonable expectation of privacy in his sent text messages and, as a result, had standing under s. 8 to challenge the Production Order.

[91] Having recognized that Mr. Jones has standing and that s. 8 is engaged, the next question is whether the search and seizure in this case was reasonable. That, in turn, depends on whether the search and seizure was authorized by law, that is, was it open to the police to obtain copies of historical text messages from a service provider pursuant to a Production Order or was a Part VI authorization required.

[92] Mr. Jones argued that obtaining historical text messages through a service provider constitutes an interception of a private communication for which a Part VI authorization is required. The Crown's argument was that "interception" in Part VI does not apply to the police requesting third party production

[3] Now s. 487.014 of the *Criminal Code*.

fondée sur l'art. 487.012 du *Code criminel*, L.R.C. 1985, c. C-46[3]. Tristin Jones avait envoyé les messages en question au compte de téléphone cellulaire Telus associé à son coaccusé. Ces messages ont constitué le fondement de la déclaration de culpabilité prononcée contre M. Jones relativement à l'infraction d'avoir offert de céder une arme à feu.

[89] Tout comme dans le pourvoi connexe *R. c. Marakah*, [2017] R.C.S. 608, la première question consiste à décider si la personne qui envoie des messages textes possède une attente raisonnable au respect de sa vie privée à l'égard des copies des messages textes qu'elle a envoyés et si, par conséquent, elle a qualité pour invoquer l'art. 8 de la *Charte canadienne des droits et libertés*, lequel est rédigé ainsi :

Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

[90] Je souscris à l'opinion de la juge Côté selon laquelle M. Jones possédait une attente raisonnable au respect de sa vie privée à l'égard des messages textes qu'il a envoyés et, par conséquent, avait qualité pour contester l'ordonnance de communication en vertu de l'art. 8.

[91] Après avoir reconnu que M. Jones a qualité pour agir et que l'art. 8 s'applique, la question suivante consiste à se demander si la fouille et la saisie étaient raisonnables en l'espèce. La réponse à cette question dépend de la réponse à la question de savoir si la fouille et la saisie étaient autorisées par la loi, c'est-à-dire s'il était possible pour les policiers d'obtenir des copies des messages textes existants auprès d'un fournisseur de services conformément à une ordonnance de communication, ou s'ils devaient obtenir une autorisation sous le régime de la partie VI.

[92] M. Jones a soutenu que le fait d'obtenir des messages textes existants par l'intermédiaire d'un fournisseur de services constitue une interception de communications privées requérant la délivrance d'une autorisation prévue à la partie VI. La Couronne a plaidé que l'« interception » visée à la

[3] Maintenant l'art. 487.014 du *Code criminel*.

of historical text messages because the concept of "interception" is prospective and involves the state interjecting itself into the communication process as it happens. Since the timing and technique of the investigative process and not the content of the information intercepted are what is relevant, the Crown maintained that a Production Order was sufficient to obtain copies of Mr. Jones' messages.

partie VI ne s'applique pas aux situations où les policiers sollicitent la production par un tiers de messages textes existants, étant donné que le concept d'« interception » a un caractère prospectif et implique que l'État s'interpose dans le processus de communication pendant qu'il se déroule. Comme ce sont la nature de la technique d'enquête utilisée et le moment où elle est mise en œuvre qui sont pertinents, et non le contenu des renseignements interceptés, la Couronne a fait valoir qu'une ordonnance de communication était suffisante pour obtenir des copies des messages de M. Jones.

[93] I agree with Mr. Jones and would allow the appeal. Historical text messages, like all text messages, are a "private communication" as defined in s. 183, found in Part VI of the *Criminal Code*. In my respectful view, the level of privacy protection afforded to private communications should be informed by the purposes underlying Part VI of the *Criminal Code* and based on the character of the communication, and not on the timing of the state's request for authorization or on technological differences between service providers. By prioritizing a temporal distinction to determine the level of privacy protection for text messages, Telus customers are left with less protection than those using other service providers who do not store copies of text messages simply because Telus stores copies of text messages that pass through its infrastructure. This means that the privacy rights of those who text depend on which service provider they use rather than the fact that they are texting as a means of privately communicating.

[93] Je souscris à la position de M. Jones et j'accueillerais le pourvoi. Un message texte existant, comme tout autre message texte, constitue une « communication privée » suivant la définition donnée à ce terme à l'art. 183, disposition qui se trouve dans la partie VI du *Code criminel*. Avec égards, le degré de protection accordée aux communications privées sur le plan du respect de la vie privée devrait reposer sur les objectifs qui sous-tendent la partie VI du *Code criminel* ainsi que sur la nature de la communication, et non sur le moment où l'État présente sa demande d'autorisation ou sur des différences d'ordre technologique existant entre les fournisseurs de services. Si on privilégie une distinction d'ordre temporel pour déterminer le degré de protection de la vie privée applicable à l'égard des messages textes, les clients de Telus se trouvent alors à bénéficier d'une protection inférieure à celle dont jouissent les clients faisant appel à d'autres fournisseurs de services qui ne conservent pas de copies des messages textes, et ce, tout simplement parce que Telus stocke des copies des messages textes qui passent par son infrastructure. Cela signifie que le droit des auteurs de messages textes au respect de leur vie privée dépend de l'identité de leur fournisseur de services, plutôt que du fait qu'ils utilisent les messages textes comme moyen de communiquer privément.

[94] At the same time, emphasizing the *historical* nature of a text message exchange distorts the fact that that exchange remains a conversation, albeit one that takes place electronically and is assigned a specific timestamp. The timing of the state's

[94] En même temps, l'accent mis sur le caractère *existant* d'un échange de messages textes dénature le fait qu'un tel échange n'en demeure pas moins une conversation, bien que celle-ci se déroule électroniquement et qu'on lui assigne une marque

request for information should not distort the communicative dimension of a text message exchange.

Analysis

[95] Production Orders were created to allow investigators to compel third parties who are not under investigation to produce data or documents that are relevant to the commission of an alleged offence (see J. A. Fontana and D. Keeshan, *The Law of Search and Seizure in Canada* (9th ed. 2015), at p. 494). A Production Order can only be obtained if the justice or judge is satisfied, in an *ex parte* application, that an offence has been or is suspected of having been committed under the *Criminal Code* or an Act of Parliament, that the documents or data would provide evidence respecting the commission of the offence, and that the person subject to the order has possession or control of the documents or data (s. 487.012(3)).[4]

[96] The Part VI authorization scheme (ss. 183 to 196), on the other hand, is in the section of the *Criminal Code* entitled "Invasion of Privacy". Part VI covers three broad categories of intercepts. This case is about the requirement for a standard intercept without consent.

[97] Part VI sets out a comprehensive scheme for the interception of private communications (*R. v. TELUS Communications Co.*, [2013] 2 S.C.R. 3, at para. 2). It is now well established that state action in the context of search and seizure, including electronic surveillance, will engage s. 8 of the *Charter* if it affects a person's reasonable expectation of privacy. As Prof. Hamish Stewart notes, "the search must be authorized by law, the law authorizing the search must be reasonable (*i.e.*, constitutionally valid), and the manner in which the search is conducted must be reasonable. A search that fails to meet any one of these three criteria is unreasonable and violates section 8" ("Normative Foundations

[4] Now s. 487.014(2) of the *Criminal Code*.

temporelle. Le moment où l'État présente sa demande d'information ne devrait pas dénaturer la dimension communicationnelle d'un échange de messages textes.

Analyse

[95] Les ordonnances de communication ont été créées afin de permettre aux enquêteurs de contraindre des tiers ne faisant pas l'objet de l'enquête à produire des données ou documents pertinents à l'égard de la perpétration de l'infraction reprochée (voir J. A. Fontana et D. Keeshan, *The Law of Search and Seizure in Canada* (9e éd. 2015), p. 494). Le juge de paix ou le juge ne peut rendre une ordonnance de communication que s'il est convaincu, au terme d'une demande présentée *ex parte*, qu'une infraction au *Code criminel* ou à une autre loi fédérale a été ou est présumée avoir été commise, que les documents ou données fourniront une preuve touchant la perpétration de l'infraction et que les documents ou les données sont en la possession de la personne en cause ou à sa disposition (par. 487.012(3))[4].

[96] Le régime d'autorisation de la partie VI (art. 183 à 196), en revanche, se trouve dans la partie du *Code criminel* intitulée « Atteintes à la vie privée ». La partie VI couvre trois grandes catégories d'interceptions. La présente affaire porte sur l'exigence relative à l'interception usuelle sans consentement.

[97] La partie VI instaure un régime complet en vue de l'interception de communications privées (*R. c. Société TELUS Communications*, [2013] 2 R.C.S. 3, par. 2). Il est maintenant bien établi que les actions de l'État en contexte de fouilles, perquisitions et saisies, y compris en matière de surveillance électronique, entraînent l'application de l'art. 8 de la *Charte* si elles ont une incidence sur l'attente raisonnable d'une personne au respect de sa vie privée. Comme l'a souligné le professeur Hamish Stewart, [TRADUCTION] « la fouille ou la perquisition doit être autorisée par la loi, la loi autorisant la fouille ou la perquisition ne doit pas être abusive (c.-à-d., elle doit être constitutionnellement valide) et la fouille

[4] Maintenant le par. 487.014(2) du *Code criminel*.

for Reasonable Expectations of Privacy" (2011), 54 *S.C.L.R.* (2d) 335, at p. 335).

[98] Section 183 sets out the definitions applicable to Part VI of the *Criminal Code*. The relevant defined terms are:

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

. . .

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

[99] The question in this appeal turns on the meaning of the term "intercept", and on whether the seizure of stored copies of historical text messages from a service provider constitutes an "intercept" within the meaning of s. 183.

[100] Compared with the other search and seizure and warrant provisions in the *Criminal Code*, including the provision dealing with Production Orders, the provisions in Part VI establish more stringent requirements before authorization is granted. *TELUS* explained the purpose behind these more onerous requirements:

These safeguards illuminate Parliament's intention that a higher degree of protection be available for private communications. Part VI has broad application

ou la perquisition ne doit pas être effectuée d'une manière abusive. Une fouille ou perquisition qui ne satisfait pas à l'un ou l'autre de ces critères est abusive et contrevient à l'article 8 » (« Normative Foundations for Reasonable Expectations of Privacy » (2011), 54 *S.C.L.R.* (2d) 335, p. 335).

[98] L'article 183 énonce les définitions applicables à la partie VI du *Code criminel*. Les définitions pertinentes sont :

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 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.

[99] La question en litige dans le présent pourvoi dépend du sens du mot « intercepter » et de la question de savoir si la saisie auprès d'un fournisseur de services de copies de messages textes existants stockées par ce dernier constitue une « interception » visée à l'art. 183.

[100] Par comparaison aux conditions prévues par les autres dispositions du *Code criminel* relatives aux fouilles, perquisitions, saisies et mandats, y compris la disposition portant sur les ordonnances de communication, les dispositions de la partie VI établissent des exigences plus strictes pour l'octroi de l'autorisation. L'arrêt *TELUS* a exposé la raison d'être de ces exigences plus sévères :

Ces garanties font bien ressortir l'intention du législateur d'accorder une protection plus grande aux communications privées. La partie VI s'applique largement

to a number of technologies and includes more rigorous safeguards than other warrant provisions in the *Code*. [para. 31]

[101] *TELUS*, guided by this purpose, rejected a narrow definition of the term "intercept". In determining whether Part VI authorization was required for the prospective, continuous, daily production of text messages from a service provider, the plurality in *TELUS* rejected a restrictive approach:

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

. . .

A 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. [Emphasis in original; paras. 33 and 35.]

[102] Notably, *TELUS* recognized that there is no requirement that the interception of a private communication be simultaneous or contemporaneous with the making of the communication:

There is no requirement in the *Code* definition of "intercept" that the interception of a private communication be simultaneous or contemporaneous with the making of the communication itself. If Parliament intended to include such a requirement, it would have included it in the definition of "intercept". Instead, it chose to adopt

à divers moyens technologiques et prévoit des garanties plus strictes que d'autres dispositions du *Code* en matière de mandat. [par. 31]

[101] L'arrêt *TELUS*, sur la base de cette raison d'être, a rejeté une définition étroite du mot « intercepter ». Dans le cadre de leur examen visant à décider si une autorisation fondée sur la partie VI était nécessaire pour obtenir d'un fournisseur de services la communication prospective de messages textes, sur une base quotidienne continue, une pluralité de juges ont rejeté le recours à une approche restrictive :

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 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). . .

. . .

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. [par. 33 et 35]

[102] En particulier, l'arrêt *TELUS* a reconnu que rien n'exige que l'interception d'une communication privée s'effectue simultanément à la communication elle-même ou sensiblement au même moment :

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

a wider definition, consistent with Part VI's purpose to offer broad protection for private communications from unauthorized interference by the state.

The interpretation of "intercept a private communication" must, therefore, focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made. 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.

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. [paras. 35-37]

[103] Moldaver J. too, in *TELUS*, concluded that 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" (para. 77). While not prepared to find that the investigative technique used by the police was in fact an "intercept", he found that it was "substantively equivalent" to an intercept and therefore required Part VI authorization (para. 77).

[104] As in *TELUS*, where the issue was whether Part VI authorization was required for prospective text messages, a technical approach to defining "intercept" should be rejected even when dealing, as we are in this case, with the stored copies of historical text messages. Requiring that the interception of a private communication be simultaneous or contemporaneous with the making of a communication itself overlooks the content and character of

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

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.

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. [par. 35-37]

[103] Le juge Moldaver, dans *TELUS*, a lui aussi conclu que le critère applicable à l'égard de 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 » (par. 77). Même s'il n'était pas disposé à conclure que la technique d'enquête utilisée par les policiers avait constitué en fait une « interception », il a jugé qu'elle correspondait, « sur le plan du fond », à une interception, et qu'elle nécessitait donc la délivrance d'une autorisation en vertu de la partie VI (par. 77).

[104] Tout comme dans *TELUS*, où la question en litige consistait à décider si une autorisation délivrée sous le régime de la partie VI était nécessaire pour obtenir la communication de futurs messages textes, il y a lieu de rejeter une approche technique afin de définir « intercepter » même dans les cas où il s'agit, comme en l'espèce, de copies stockées de messages textes existants. Le fait d'exiger que l'interception d'une communication privée s'effectue

text messaging while neutering Part VI's ability to protect the right to privacy in new, electronic and text-based technologies.

[105] The only difference between *TELUS*, dealing with prospective text messages, and this case, dealing with historical text messages, is the timing of the state's request for authorization. This was reinforced by the intervener Criminal Lawyers' Association of Ontario in its factum where it said that, "[t]echnologically speaking, [*TELUS*] and [Mr. Jones'] case are identical: a private communication is made, it is then stored on the company's computer, and then the state acquires it" (para. 16). If the term "intercept" in s. 183 is interpreted in the context of the broader Part VI scheme and the purpose that it is meant to serve, namely, to prevent the state acquisition of private communications without lawful authorization and to protect the privacy interests inherent in the content of private communications, then the Part VI protections should not fluctuate with the timing of the state's interception of a private communication. As noted in *TELUS*, interpreting the phrase "intercept[ion] [of] a private communication" must "focus on the acquisition of informational content and the individual's expectation of privacy at the time the communication was made" (para. 36).

[106] In other words, the focus must remain on the substance of what the state seeks to obtain. When the police obtain copies of text messages from a service provider, they are acquiring a complete record of all electronic conversations that took place during a given period. In both *TELUS* and this case, the informational content acquired by the state is the same: a complete record of all private communications in the given period. A singular focus on the *historical* dimension of the record should not detract from the content and character of

simultanément à la communication elle-même ou sensiblement au même moment ne tient pas compte du contenu et de la nature du message texte, en plus de neutraliser la capacité de la partie VI de protéger le droit au respect de la vie privée des personnes utilisant des nouveaux moyens technologiques de communication textuelle électronique.

[105] La seule différence entre l'affaire *TELUS*, qui concernait des messages textes futurs, et celle qui nous occupe, qui porte sur des messages textes existants, est le moment de la présentation de la demande d'autorisation par l'État. L'intervenante la Criminal Lawyers' Association of Ontario a insisté sur ce point dans son mémoire, affirmant ce qui suit : [TRADUCTION] « Sur le plan de la technologie, [*TELUS*] et l'affaire [de M. Jones] sont identiques : une communication privée a lieu, elle est stockée sur l'ordinateur de l'entreprise, puis l'État en prend connaissance » (par. 16). Si le mot « intercepter » à l'art. 183 est interprété dans le contexte général du régime de la partie VI et de l'objet que celui-ci est censé viser, c'est-à-dire prévenir la prise de connaissance par l'État de communications privées sans autorisation valable et protéger le droit intrinsèque au respect de la vie privée à l'égard du contenu de communications privées, alors les protections qu'offre la partie VI ne devraient pas fluctuer en fonction du moment où l'État intercepte une communication privée. Comme il a été souligné dans l'arrêt *TELUS*, il faut interpréter les mots « intercept[ion] [d']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 » (par. 36).

[106] Autrement dit, il faut continuer à mettre l'accent sur la substance de ce que l'État cherche à obtenir d'un fournisseur de services. Lorsque les policiers obtiennent d'un fournisseur de services des copies de messages textes, ils prennent connaissance d'un relevé complet de l'ensemble des conversations électroniques qui ont eu lieu au cours d'une période donnée. Tant dans *TELUS* qu'en l'espèce, le contenu informationnel dont prend connaissance l'État est le même : un relevé complet de l'ensemble des communications privées survenues au cours d'une

this record. It is a record of a conversation that took place between individuals, albeit in an electronic format, that has been assigned a specific timestamp. This record may capture electronic conversations between several people innocently participating in an electronic conversation with the targeted recipient, as well as electronic conversations involving multiple participants engaged in a group text. Clearly, by obtaining copies of historical text messages, the state is acquiring more than mere "documents" or "data", as it does under a Production Order, it is obtaining records of "electronic conversations":

> Text messaging is, in essence, an electronic conversation. The only practical difference between text messaging and the traditional voice communications is the transmission process. [*TELUS*, at para. 5]

[107] Simpson J. outlined the breadth of information obtained when the state seeks copies of historical text messages from a service provider in *R. v. Hoelscher*, 2016 ABQB 44:

> When the police obtain a search warrant for an actual cell phone of a sender or a recipient of a text message, the police only acquire what remains preserved of a communication on the cell phone. They might not acquire everything an individual has sent or received. In order to protect certain private communications from unwanted intrusions, a sender or recipient might delete the message, go a step further and electronically clear the information or go so far as to destroy the cell phone.
>
> However, when police intercept text messages from a service provider, they acquire every message sent and received for the phone number, for a specific period of time. The owner of the cell phone has no control over the storage or disposition of the messages by the service provider.

période donnée. L'insistance particulière sur le fait que le relevé porte sur des messages textes *existants* ne devrait pas faire oublier le contenu et la nature de ce relevé. Il s'agit d'un relevé reproduisant le texte d'une conversation qui a eu lieu entre des personnes, même si elle a pris une forme électronique, et à laquelle on a assigné un repère temporel précis. Ce relevé pourrait comprendre des conversations électroniques entre plusieurs personnes qui participent innocemment à une conversation électronique avec le destinataire visé, ainsi que des conversations électroniques entre de multiples participants à un échange de messages textes au sein d'un groupe. Manifestement, en obtenant des copies des messages textes existants, l'État ne prend pas connaissance uniquement de simples « documents » ou « données », comme il le fait en vertu d'une ordonnance de communication, il obtient l'enregistrement de « conversations électroniques » :

> 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. [*TELUS*, par. 5]

[107] Dans *R. c. Hoelscher*, 2016 ABQB 44, le juge Simpson a expliqué l'ampleur des renseignements obtenus lorsque l'État cherche à obtenir d'un fournisseur de services des copies de messages textes existants :

> [TRADUCTION] Lorsque les policiers obtiennent un mandat de perquisition visant le téléphone cellulaire lui-même de l'expéditeur ou du destinataire d'un message texte, ils prennent connaissance uniquement de ce qui reste de la communication dans le téléphone cellulaire. Ils ne seront peut-être pas en mesure de prendre connaissance de tous les messages que la personne concernée a envoyés ou reçus. Afin de protéger certaines communications privées contre les intrusions non désirées, l'expéditeur ou le destinataire peut supprimer le message, aller un peu plus loin et effacer électroniquement les données ou encore même aller jusqu'à détruire le téléphone cellulaire.
>
> Cependant, lorsque les policiers interceptent des messages textes passant par un fournisseur de services, ils prennent connaissance de tous les messages envoyés à partir du numéro de téléphone et reçus à ce numéro pendant une période précise. Le propriétaire du téléphone cellulaire n'a aucun contrôle sur la conservation ou la destruction des messages par le fournisseur de services.

The acquisition of information from the service provider can therefore be distinguished from the acquisition of information from the sender's cell phone or the recipient's cell phone, as in those cases, the respective individuals have some control over the information present on the cell phone. This loss of control of a private communication in the hands of the service provider, and the serious level of intrusion justify the protections of Part VI. [paras. 113-15 (CanLII)]

La prise de connaissance de renseignements obtenus auprès du fournisseur de services se distingue donc de la prise de connaissance de renseignements à partir du téléphone cellulaire de l'expéditeur ou du destinataire, en ce que, dans le second cas, ces derniers exercent un certain contrôle sur les renseignements se trouvant dans le téléphone cellulaire. Cette perte de contrôle sur une communication privée en la possession du fournisseur de services et le degré d'intrusion considérable en cause justifient les mesures de protection prévues à la partie VI. [par. 113-115 (CanLII)]

[108] Emphasizing the historical nature of a text message subjects the privacy rights of text message participants to the technical differences between service providers. *TELUS* recognized that technological developments that allow the state to acquire copies of prospective text messages should not determine the scope of the protection afforded to those private communications. It seems to me difficult to make a different argument for historical messages. In other words, technological tools that allow the state to obtain copies of historical text messages from service providers should not determine the scope of protection afforded to them.

[108] Le fait de mettre l'accent sur le caractère existant des messages textes visés fait dépendre le droit des participants à ces messages au respect de leur vie privée des différences techniques qui existent entre les fournisseurs de services. Dans *TELUS*, il a été jugé que l'existence de progrès technologiques qui permettent à l'État de prendre connaissance de copies de messages textes futurs ne devrait pas déterminer l'étendue de la protection accordée à ces communications privées. Il me semble difficile de formuler une conclusion différente pour les messages existants. En d'autres mots, les outils technologiques qui permettent à l'État d'obtenir des copies de messages textes existants auprès de fournisseurs de services ne devraient pas déterminer l'étendue de la protection accordée à ces messages.

[109] The logical extension of all of this, in my respectful view, whether one finds that the technique used here to acquire copies of historical text messages was an intercept, or "substantively equivalent" to an intercept, is the following, as Burrows J. explained in *R. v. Croft*, 304 C.C.C. (3d) 279 (Alta. Q.B.):

[109] La conséquence logique de tout cela, que l'on arrive à la conclusion que la technique utilisée en l'espèce pour prendre connaissance des copies de messages textes existants constituait une interception, ou qu'elle était « équivalente sur le fond » à une interception, est la suivante, qu'a expliquée le juge Burrows dans *R. c. Croft*, 304 C.C.C. (3d) 279 (B.R. Alb.) :

. . . if one accepts that to prospectively authorize the acquisition of text messages anticipated to be recorded is to authorize the interception of private communications . . . to authorize the acquisition of text messages previously recorded in Telus' transmission infrastructure must also be to authorize the interception of private communications. [para. 47]

[TRADUCTION] . . . si l'on accepte que le fait d'autoriser prospectivement la prise de connaissance de messages textes qui, prévoit-on, seront enregistrés consiste à autoriser l'interception de communications privées [. . .] le fait d'autoriser la prise de connaissance de messages textes déjà enregistrés dans l'infrastructure de Telus consiste également à autoriser l'interception de communications privées. [par. 47]

[110] Simpson J. made a similar point in *Hoelscher*:

[110] Le juge Simpson a exprimé un point de vue semblable dans *Hoelscher* :

. . . it is important to remember that the acquisition by the police of text messages stored by a service provider, whether by way of a retrospective or prospective authorization, will never occur simultaneously or contemporaneously with the sending of the message. A retrospective authorization will of course always make for the acquisition of stored material. It cannot occur simultaneously with the sending of the text message. Similarly when the police, with a prospective authorization, exploit the storage system of Telus, then the information is always stored before the police acquire it.

. . .

In this case, the police seek to acquire the content of a recorded telecommunications from the transmission service provider. It does not matter whether the police request the authorization one week before the text is sent, one minute before it is sent, or one week after it is sent, in all instances it is the acquisition of a private telecommunication from a service provider, and it is the content of those communications Part VI aims to protect. The acquisition of the content from the service provider is the interception, not the time which the police request the authorization. [paras. 100 and 103]

[111] A text message cannot be sent without passing through a service provider. Increasing reliance on text messaging is resulting in "new and rather rich sources of evidentiary material for criminal investigators", generating new privacy concerns (*R. v. Carty*, 2014 ONSC 212 (Boswell J.), at para. 9; see also para. 11 (CanLII)). The intervener British Columbia Civil Liberties Association aptly explained the implications of increasing reliance on texting in its factum: "Canadians are increasingly communicating by text messaging. . . . [M]uch of what was once available to the police only through a 'wiretap' (authorized under Part VI) is now available through the acquisition of text messages from a computer" (para. 3).

[TRADUCTION] . . . il est important de se rappeler que la prise de connaissance par les policiers de messages textes stockés par un fournisseur de services — que ce soit au moyen d'une autorisation rétrospective ou prospective — ne s'effectue jamais simultanément à l'envoi du message ou sensiblement au même moment. Une autorisation rétrospective aboutit évidemment toujours à la prise de connaissance de documents stockés. La prise de connaissance ne peut avoir lieu simultanément à l'envoi du message texte. De la même façon, lorsque les policiers, au moyen d'une autorisation prospective, tirent profit du système de stockage de Telus, les renseignements sont toujours stockés avant que les policiers n'en prennent connaissance.

. . .

En l'espèce, les policiers demandent à prendre connaissance du contenu d'une télécommunication enregistrée par un fournisseur de services de transmission. Il importe peu qu'ils demandent l'autorisation une semaine ou une minute avant que le message texte soit envoyé ou une semaine après, il s'agit dans tous les cas de la prise de connaissance de télécommunications privées d'un fournisseur de services, et la partie VI vise à protéger le contenu de ces communications. La prise de connaissance du contenu demandé auprès du fournisseur de services constitue l'interception, celle-ci ne dépend pas du moment où la police demande l'autorisation. [par. 100 et 103]

[111] Un message texte ne peut être envoyé sans passer par un fournisseur de services. L'utilisation sans cesse croissante par les gens des messages textes se traduit par [TRADUCTION] « de nouvelles sources particulièrement riches d'éléments de preuve pour les enquêteurs criminels », situation qui soulève de nouvelles préoccupations en matière de respect de la vie privée (*R. c. Carty*, 2014 ONSC 212 (le juge Boswell), par. 9; voir aussi le par. 11 (CanLII)). L'intervenante la British Columbia Civil Liberties Association a bien expliqué les conséquences du recours accru aux messages textes dans son mémoire : [TRADUCTION] « Les Canadiens communiquent de plus en plus par messages textes. [. . .] [B]ien des éléments que les policiers ne pouvaient jusque-là recueillir que par voie d'"écoute électronique" (mesure autorisée en vertu de la partie VI) peuvent maintenant être recueillis en prenant connaissance de messages textes se trouvant dans un ordinateur » (par. 3).

[112] Telus, it seems, is the only service provider to store copies of text messages for a period of time. As Moldaver J. noted in his reasons in *TELUS*, "[t]he fact that Telus stores its subscribers' text messages in this manner is significant . . . because it creates an investigative resource for the authorities" (para. 59), an investigative resource that is not available through the other service providers who do not store copies of text messages.

[113] In this case, the police obtained several Production Orders pursuant to s. 487.012 of the *Criminal Code* directed at the service providers Bell, Rogers and Telus. Only Telus stored the content of incoming and outgoing text messages for a period of time after the messages were sent and received. No text messages were obtained from accounts held with the other service providers. Telus' unique storage practices, rather than the underlying principles in Part VI, led to the production of copies of historical text messages from the targeted Telus account, and the loss of Mr. Jones' privacy protections available under Part VI of the *Criminal Code*. Again, the applicability of Part VI should depend on the substance of what the investigative technique seeks to access, not on the timing of when access is sought, or on the vagaries of the service provider's technological practices.

[114] Since no Part VI authorization was obtained, the acquisition of copies of Mr. Jones' historical text messages through the Production Order was invalid and breached his rights under s. 8 of the *Charter*.

[115] The remaining issue is whether the improperly obtained evidence should be excluded under s. 24(2) of the *Charter* in accordance with this Court's decision in *R. v. Grant*, [2009] 2 S.C.R. 353. In my respectful view, on balance, the admission of the historical text message evidence obtained pursuant to the Production Order would bring the administration of justice into disrepute.

[112] Telus, semble-t-il, est le seul fournisseur de services qui conserve des copies des messages textes pendant une certaine période. Comme l'a souligné le juge Moldaver dans les motifs qu'il a exposés dans l'arrêt *TELUS*, « [l]e fait que Telus conserve les messages textes de ses abonnés de cette façon est important [. . .] parce qu'il crée une ressource d'enquête pour les autorités » (par. 59), une ressource d'enquête qui n'est pas disponible auprès des autres fournisseurs de services, lesquels ne conservent pas de copies des messages textes.

[113] En l'espèce, les policiers ont obtenu, en vertu de l'art. 487.012 du *Code criminel*, plusieurs ordonnances de communication visant les fournisseurs de services Bell, Rogers et Telus. Seule la société Telus conserve pendant une certaine période le contenu des messages textes envoyés et reçus par ses abonnés. Aucun message texte n'a été obtenu à partir de comptes existants auprès des autres fournisseurs de services. Ce sont les pratiques de stockage uniques à Telus, plutôt que les principes qui sous-tendent la partie VI, qui ont mené à la communication des copies de messages textes existants du compte Telus visé, et à la perte par M. Jones des mesures de protection de la vie privée prévues par la partie VI du *Code criminel*. Encore une fois, l'applicabilité de la partie VI devrait dépendre de la substance des éléments auxquels la technique d'enquête vise à obtenir accès, et non du moment où cet accès est demandé, ou encore du hasard des pratiques technologiques des fournisseurs de services.

[114] Comme aucune autorisation fondée sur la partie VI n'a été obtenue, la prise de connaissance des copies des messages textes existants de M. Jones obtenues au moyen de l'ordonnance de communication était invalide et violait les droits garantis à ce dernier par l'art. 8 de la *Charte*.

[115] Il reste à décider si la preuve obtenue de façon irrégulière devrait être écartée en vertu du par. 24(2) de la *Charte*, conformément à l'arrêt de notre Cour *R. c. Grant*, [2009] 2 R.C.S. 353. Tout compte fait, je suis d'avis que l'utilisation en preuve des messages textes existants obtenus en application de l'ordonnance de communication serait susceptible de déconsidérer l'administration de la justice.

[116] The public's interest in seeing a determination on the merits is balanced against its interest in "having a justice system that is above reproach" (*Marakah*, at para. 72, per McLachlin C.J., quoting *Grant*, at para. 84). As Brown J. noted in *R. v. Paterson*, [2017] 1 S.C.R. 202: "It is . . . important not to allow . . . society's interest in adjudicating a case on its merits to trump all other considerations . . ." (para. 56).

[117] The impact of the *Charter*-infringing conduct on Mr. Jones' *Charter*-protected privacy interests under s. 8 of the *Charter* was significant. Whether they take the form of a historical record or occur in real-time, electronic conversations have the potential to reveal information going to the individual's biographical core, including information which tends to reveal intimate details of the lifestyle or personal choices of an individual. In the companion case of *Marakah*, Chief Justice McLachlin emphasized that Mr. Marakah "had a considerable, *Charter*-protected privacy interest in his . . . electronic conversation" (para. 67). Similarly, Mr. Jones had a considerable, *Charter*-protected privacy interest in his electronic conversation with the recipient of his text messages. As Cromwell J. noted in *R. v. Côté*, [2011] 3 S.C.R. 215:

> . . . it must not be forgotten that the purpose of the *Charter*'s protection against unreasonable searches is to prevent them before they occur, not to sort them out from reasonable intrusions on an *ex post facto* analysis: *R. v. Feeney*, [1997] 2 S.C.R. 13, at para. 45. Thus, prior authorization is directly related to, and forms part of, an individual's reasonable expectation of privacy. [para. 84]

[118] I acknowledge that the police did not, technically, act in bad faith, but I cannot accept that the failure to seek Part VI authorization did not put public confidence in the administration of justice at serious risk. The evolution of shifting technology has resulted in a correspondingly evolving jurisprudence which tries to keep pace with the impact of technology on constitutional rights. Where no

[116] L'intérêt du public à ce qu'un jugement au fond soit rendu est mis en balance avec son intérêt « en l'irréprochabilité du système de justice » (*Marakah*, par. 72, la juge en chef McLachlin, citant *Grant*, par. 84). Comme l'a mentionné le juge Brown dans *R. c. Paterson*, [2017] 1 R.C.S. 202 : « Il importe [. . .] de ne pas permettre que [. . .] l'intérêt de la société dans l'instruction de l'affaire au fond l'emporte sur toutes les autres considérations . . . » (par. 56).

[117] Les répercussions de la conduite attentatoire à la *Charte* sur le droit à la protection de la vie privée garanti à M. Jones par l'art. 8 de ce texte ont été importantes. Qu'il s'agisse de messages existants ou d'un échange en temps réel, les conversations électroniques sont susceptibles de révéler des renseignements biographiques sur les gens, notamment des renseignements qui tendent à révéler des détails intimes sur leur mode de vie et leurs choix personnels. Dans le pourvoi connexe *Marakah*, la juge en chef McLachlin a souligné que M. Marakah « avait [. . .] un important droit au respect de sa vie privée reconnu par la *Charte* dans la conversation électronique qu'il avait eue » (par. 67). Tout comme ce dernier, M. Jones avait en vertu de la *Charte* un important droit au respect de sa vie privée à l'égard de sa conversation électronique avec le destinataire de ses messages textes. Comme l'a souligné le juge Cromwell dans *R. c. Côté*, [2011] 3 R.C.S. 215 :

> Il faut [. . .] se garder d'oublier que l'objet de la garantie constitutionnelle contre les fouilles et les perquisitions abusives est de faire obstacle à ces dernières, et non de les distinguer d'atteintes non abusives dans le cadre d'une analyse *ex post facto* : *R. c. Feeney*, [1997] 2 R.C.S. 13, par. 45. L'autorisation préalable est donc directement liée à l'attente raisonnable d'une personne en matière de vie privée et elle en fait partie intégrante. [par. 84]

[118] Je reconnais que, techniquement, la police n'a pas agi de mauvaise foi, mais je ne peux accepter que le défaut d'obtenir une autorisation sous le régime de la partie VI n'a pas sérieusement compromis la confiance du public envers l'administration de la justice. L'évolution rapide de la technologie entraîne une évolution correspondante de la jurisprudence, laquelle s'efforce de suivre le rythme de

case directly on point has been decided, the police have two choices: to use the jurisprudential gap as a rationale for being more intrusive, or to exercise greater caution before interfering with legislatively endorsed privacy rights. It seems to me that the better judicial approach is one that encourages conduct on the part of the police that errs on the side of being protective of the rights of the public, rather than one that endorses *Charter* breaches in deference to the mechanics of new technologies.

[119] I would therefore exclude the text message evidence obtained through the Production Order and set aside the conviction.

Appeal dismissed, ABELLA J. *dissenting.*

Solicitors for the appellant: Fasken Martineau DuMoulin, Ottawa; Lyttle McGarry Del Greco, Ottawa.

Solicitor for the respondent Her Majesty The Queen in Right of Canada: Public Prosecution Service of Canada, Toronto.

Solicitor for the respondent Her Majesty The Queen in Right of Ontario: Attorney General of Ontario, Toronto.

Solicitor for the intervener the Attorney General of British Columbia: Attorney General of British Columbia, Victoria.

Solicitor for the intervener the Director of Criminal and Penal Prosecutions: Director of Criminal and Penal Prosecutions, Montréal.

Solicitors for the intervener the Criminal Lawyers' Association of Ontario: Ursel Phillips Fellows Hopkinson, Toronto.

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

l'incidence de la technologie sur les droits garantis par la Constitution. Dans les cas où aucune décision portant exactement sur une situation litigieuse n'a encore été rendue, les policiers ont alors le choix entre deux possibilités : utiliser la lacune dans la jurisprudence pour justifier une conduite plus envahissante, ou exercer davantage de précaution avant de porter atteinte à des droits protégeant la vie privée garantis par la loi. Il me semble que la meilleure approche à adopter par les tribunaux consiste à inciter les policiers à pécher par excès de prudence afin de protéger les droits du public, plutôt qu'à cautionner des violations de la *Charte* par déférence pour la mécanique des nouvelles technologies.

[119] Par conséquent, j'écarterais les messages textes obtenus au moyen de l'ordonnance de communication et j'annulerais la déclaration de culpabilité.

Pourvoi rejeté, la juge ABELLA *est dissidente.*

Procureurs de l'appelant : Fasken Martineau DuMoulin, Ottawa; Lyttle McGarry Del Greco, Ottawa.

Procureur de l'intimée Sa Majesté la Reine du chef du Canada : Service des poursuites pénales du Canada, Toronto.

Procureur de l'intimée Sa Majesté la Reine du chef de l'Ontario : Procureur général de l'Ontario, Toronto.

Procureur de l'intervenant le procureur général de la Colombie-Britannique : Procureur général de la Colombie-Britannique, Victoria.

Procureur de l'intervenant le directeur des poursuites criminelles et pénales : Directeur des poursuites criminelles et pénales, Montréal.

Procureurs de l'intervenante Criminal Lawyers' Association of Ontario : Ursel Phillips Fellows Hopkinson, Toronto.

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

Solicitors for the intervener the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: Presser Barristers, Toronto; Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, Ottawa.

Solicitors for the intervener the British Columbia Civil Liberties Association: Stockwoods, Toronto.

Procureurs de l'intervenante la Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko : Presser Barristers, Toronto; Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko, Ottawa.

Procureurs de l'intervenante British Columbia Civil Liberties Association : Stockwoods, Toronto.