SUPREME COURT OF CANADA

CITATION: R. *v.* Jones, 2017 SCC 60

APPEAL HEARD: March 23, 2017
JUDGMENT RENDERED: December 8, 2017
DOCKET: 37194

BETWEEN:

Tristin Jones
Appellant

and

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

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

REASONS FOR JUDGMENT: (paras. 1 to 82)	Côté J. (McLachlin C.J. and Moldaver, Karakatsanis and Gascon JJ. concurring)
CONCURRING REASONS: (paras. 83 to 87)	Rowe J.
DISSENTING REASONS: (paras. 88 to 119)	Abella J.

R. *v.* JONES

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 — 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 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 deprive 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 encompasses the production or seizure 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). 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).

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 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 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 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 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.

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; *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 947, 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.

By Abella J. (dissenting)

R. v. Marakah, 2017 SCC 59; *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 (l)(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 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 J. was delivered by

CÔTÉ J. —

I. Overview

[1] The appellant, Mr. Jones, 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 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 (the

"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 cell phone subscription.

[3] Telus complied with the Production Order and provided the requested records to the police. The records revealed a text message exchange (the "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 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 convicted of several firearms trafficking and drug trafficking offences.

[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.

[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?

[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 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).

[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;

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

(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, 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 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 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.

[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".

[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.

[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.

[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 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 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, 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 947, 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 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 (transcript, at p. 137). 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

[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.

and the Crown, it is more fitting that the Crown be restrained from adopting inconsistent positions.

[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 cell phone 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" (*R. v. White*, [1999] 2 S.C.R. 417, at para. 41). Like section 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 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, A.R., vol. I, at pp. 1-41, at para. 31 (vii)). 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.

(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 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 deprive 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*, 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 para. 17; *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, 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.

[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. [Emphasis added.]
>
> (*Spencer*, at para. 62)

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

> . . . telecommunications service providers act merely as a third-party "conduit" for the transmission of private communications and ought to be able to provide services without having a legal effect on the nature (or, in this case, the protection) of these communications . . . . [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 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*.

[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.

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

[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.

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

(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 cell phone 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 (C.A.) 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' 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 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" (*TELUS*, at 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 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 investigate technologies and their impact on citizens' privacy, not the protection of private communications at large. As explained below, 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 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 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 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).

[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), 490.5(l)(c). The distinct translation here suggests a different meaning than in those other contexts.

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

(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 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). 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 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.

[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).

[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).

[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* 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 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

ROWE J. —

[83] 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.

[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": at 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.

[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.

[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.

The following are the reasons delivered by

ABELLA J. —

[88] The police obtained copies of historical text messages through a Production Order pursuant to s. 487.012 of the *Criminal Code*, R.S.C. 1985, c. C-46.[3] Tristin Jones sent these messages to the Telus cell phone account associated with his

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

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 SCC 59, 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 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.

[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 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.

[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 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

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

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 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 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 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.

[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 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" (I.F., at 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 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 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.
>
> 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. 113-115 (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.

[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*, 2013 ABQB 640, 304 C.C.C. (3d) 279:

> . . . 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]

[110] Simpson J. made a similar point in *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. . . . much 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" (I.F., at para. 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.

[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: "[i]t 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 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.

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.