

Her Majesty the Queen v. Telus Communications Company

[Indexed as: R. v. Telus Communications Co.]

2011 ONSC 1143

Superior Court of Justice, Sproat J. March 4, 2011

Criminal law — Search and seizure — General warrant — General warrant requiring telecommunications company to produce all text messages sent and received by two subscribers on daily basis for 30 days following issuance of warrant — Telecommunications company asserting order amounting to wiretap requiring daily authorization under provisions for intercepted private communications — General warrant not effectively authorizing interception of private communications — “Interception” requiring real-time capture of otherwise transient communications — General warrant directed to text messages stored in company’s computer database — Police not required to apply for wiretap authorization to obtain text messages — General warrant available as investigative technique of prospective daily production of text messages cannot be authorized under any other statutory provision.

The police obtained a General Warrant and Assistance Order requiring the applicant telecommunications company to produce all text messages sent and received by two subscribers for 30 days following the issuance of the order. The applicant applied to quash the general warrant, arguing that it purported to authorize the interception of private communications, so that the police were required to obtain a wiretap authorization under Part VI of the *Criminal Code*, R.S.C. 1985, c. C-46 for each day’s communications and that a general warrant was not available given the availability of orders under the wiretap provisions, the police could have applied for conventional warrants to obtain the information sought.

Held, the application should be granted in part.

The Crown conceded that to the extent that the general warrant sought production of records in existence prior to the date on which it was issued, it should be rescinded.

The general warrant did not purport to authorize the interception of private communications. “Interception” requires the real-time capture of otherwise transient communications. The applicant routinely copied all text messages and stored them in a database for at least 30 days. The general warrant was directed to the text messages stored in the applicant’s database. The police were not required to apply for a wiretap authorization in order to obtain the text messages. A general warrant was available as the investigative technique or procedure of prospective and daily production of text messages cannot be authorized under any other statutory provision. It would have been impractical for the police to obtain a daily wiretap warrant to achieve the investigative objective of obtaining stored text messages for daily review.

R. v. Brooks, [2003] O.J. No. 3757, 176 O.A.C. 337, 178 C.C.C. (3d) 361, 15 C.R. (6th) 319, 111 C.R.R. (2d) 279, 59 W.C.B. (2d) 215 (C.A.); *R. v. Ha* (2009), 96 O.R. (3d) 751, [2009] O.J. No. 1693, 2009 ONCA 340, 249 O.A.C. 43, 65 C.R. (6th) 24, 245 C.C.C. (3d) 546, 191 C.R.R. (2d) 212; *R. v. McQueen*, [1975] A.J. No. 342,

[1975] 6 W.W.R. 604, 25 C.C.C. (2d) 262 (C.A.); *R. v. Noseworthy* (1997), 33 O.R. (3d) 641, [1997] O.J. No. 1946, 100 O.A.C. 76, 116 C.C.C. (3d) 376, 43 C.R.R. (2d) 313, 34 W.C.B. (2d) 523 (C.A.); *R. v. Tele-Mobile Co.* (2008), 92 O.R. (3d) 478, [2008] 1 S.C.R. 305, [2008] S.C.J. No. 12, 2008 SCC 12, 229 C.C.C. (3d) 417, 77 W.C.B. (2d) 103, J.E. 2008-709, EYB 2008-131420, 235 O.A.C. 369, 372 N.R. 157, 55 C.R. (6th) 1, 291 D.L.R. (4th) 193, **consd**

Other cases referred to

Application under s. 83.28 of the Criminal Code (Re), [2004] 2 S.C.R. 248, [2004] S.C.J. No. 40, 2004 SCC 42, 240 D.L.R. (4th) 81, 322 N.R. 205, [2005] 2 W.W.R. 605, 199 B.C.A.C. 45, 33 B.C.L.R. (4th) 195, 184 C.C.C. (3d) 449, 21 C.R. (6th) 82, 121 C.R.R. (2d) 1, 61 W.C.B. (2d) 217; *R. v. Alvarez*, [2009] O.J. No. 3825, 2009 CarswellOnt 5448 (S.C.J.); *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, 77 W.C.B. (2d) 469; *R. v. Wilson*, [1983] 2 S.C.R. 594, [1983] S.C.J. No. 88, 4 D.L.R. (4th) 577, 51 N.R. 321, [1984] 1 W.W.R. 481, J.E. 84-70, 26 Man. R. (2d) 194, 9 C.C.C. (3d) 97, 37 C.R. (3d) 97, 11 W.C.B. 200; *United States v. Councilman*, 418 F.3d 67, 2005 U.S. App. LEXIS 16803, 36 Comm. Reg. (P & F) 737 (1st Cir. 2005)

Statutes referred to

Canadian Charter of Rights and Freedoms
Criminal Code, R.S.C. 1985, c. C-46, Part VI [as am.], ss. 183, 184(1), (2) [as am.], 185 [as am.], 186(1), 487 [as am.], 487.01, (1), (c), 487.012, (1), 492.2, (1), (2)
Federal Wiretap Act, 18 U.S.C., c. 119

Authorities referred to

Hutchison, Scott C., *Canadian Search Warrant Manual 2005* (Toronto: Thomson Carswell, 2004)
 Sullivan, Ruth, *Sullivan and Driedger on the Construction of Statutes*, 4th ed. (Markham, Ont.: Butterworths, 2002)

APPLICATION to quash a general warrant.

Tom Andreopoulos and Lisa Mathews, for respondent.
Brian Gover and Brennagh Smith, for applicant.

SPROAT J.: —

Introduction

[1] Telus applies to quash a General Warrant and Assistance Order (the “General Warrant”) by which it was obliged to produce, on a prospective daily basis, all text messages sent and received by two Telus subscribers as well as related subscriber information.

[2] It is common ground that the requirements of the General Warrant are highly unusual. In the past few years, Telus has received on the order of 10,000 search warrants and production orders. Only six have been in the form of this General Warrant. All other orders have either been production orders for retrospective production or authorizations to intercept private

communications for prospective production. Telus, therefore, challenges the General Warrant in what amounts to a test case.

[3] The principal argument advanced by Mr. Gover on behalf of Telus is that the General Warrant purports to authorize the interception of private communications. As such, a general warrant is not available and the police should have applied for what is commonly referred to as a wiretap authorization under Part VI of the *Criminal Code*, R.S.C. 1985, c. C-46. Mr. Gover further submitted that a general warrant is not available given that the police could have applied for conventional warrants to obtain the information sought.

[4] The principal argument advanced by Ms. Mathews on behalf of the Crown is that the General Warrant does not require the interception of private communications because Telus routinely stores copies of all text messages sent and received on its servers. As such, the General Warrant is directed to data that is stored and not real-time communications from sender to receiver. Ms. Mathews further argued that a general warrant is available as conventional warrants would not have permitted the investigative technique embodied in the General Warrant.

[5] Telus also argued that, given the high expectation of privacy in text messages, it was not in the best interests of the administration of justice for the General Warrant to issue. Instead, the police should have been required to apply for a wiretap authorization. Telus also cited a number of aspects of the General Warrant which Telus submitted are unwieldy and unworkable and which imposed an undue financial burden on it.

[6] The position of the Crown is that the *Criminal Code* permitted the police to obtain the General Warrant and that administrative cost and inconvenience are not grounds to set aside the General Warrant.

[7] The General Warrant was issued by Thompson J., of the Superior Court of Justice, presiding in Owen Sound. For reasons that are not material to this application, it was determined that this application should be heard by a judge presiding in Brampton.

The Evidence

Introduction

[8] Telus filed the affidavit of Don Calpito explaining how text messaging works and the affidavits of Corinne McNish and Ephry Mudryk regarding this particular General Warrant. The Crown did not seek to cross-examine. On consent, certain agreed

facts concerning the number of court orders received by Telus and the typical form of such orders were set out in a December 13, 2010 letter from Mr. Gover. The essential facts are, therefore, not in dispute.

How text messaging works

[9] The Calpito affidavit, as summarized in the Telus factum, explains the following:

27. Text messaging (known more formally as Short Message Service (“SMS”)) is a form of communication service using standardized communications protocols and mobile telephone networks to allow for the exchange of short text messages from one mobile phone device to another.

28. Text messages are always delivered using a cellular phone network. However, many phone companies now permit the initiation of text messages using the Internet.

.

30. Today, many people use text messaging as a means of communicating. The popularity of text messaging, particularly as opposed to voice telephone calls, has risen steadily in the past decade. Text messaging tends to be a less expensive alternative to voice calls, particularly during peak daytime hours.

.

34. When a cellular phone is turned on, it is constantly exchanging information with a cell phone tower over a pathway called a control channel. The control channel also provides the pathway for SMS messages.

35. When the send button is pressed on the mobile device, the text message (SMS) is sent to the cell tower emitting the strongest signal, and then routed to a Mobile Switching Center (“MSC”). The MSC is the servicing switch, which is the computerized mainframe to the network where the mobile device is registered.

36. Located within the MSC is a Short Message Service Center (“SMSC”). A SMSC is responsible for handling the SMS operations of a wireless network. The SMSC utilizes routing engines for the forward capabilities of SMS services. When the message is received at the SMSC, the SMSC will use routing engines to attempt to deliver the message to its destination.

.

38. Where the destination phone is not available (for example, it is turned off or does not have service reception), the text message will remain in the TELUS SMSC until the recipient phone is available. If the recipient phone has not become available after five days, then TELUS will delete that message from its SMSC. In those circumstances, the sender does not receive a message from TELUS that the message was not delivered.

[10] In addition to this routing of text messages as they are sent and received, all text messages are routinely copied and stored in a database for at least 30 days for what Telus describes

as troubleshooting purposes or to better deal with customer complaints. In this regard,

- (a) all text messages sent by a Telus subscriber are copied when they arrive at the Telus SMSC and the copy is forwarded to a database;
- (b) all text messages received by a Telus customer are copied and the copy is forwarded to the databases when the Telus subscriber's phone receives the message from the Telus SMSC.

The General Warrant

[11] The General Warrant was issued on March 27, 2010. The *Criminal Code* provides that a general warrant is not available if any other statutory provision provides for the type of order sought. As such, the Crown conceded that to the extent that the General Warrant sought production of records in existence prior to March 27, 2010, it should be rescinded.

[12] The General Warrant named two Telus subscribers and their telephone numbers. It required Telus to provide to the police, on a daily basis, all text messages sent to or from the two Telus subscribers as well as subscriber information identifying the individuals who sent text messages to, or received text messages from, these subscribers. The General Warrant required production by Telus over a 14-day period. The first requirement was that on March 30, 2010, Telus produce documents and information for the period March 18-30, 2010. For the 13 days following the daily requirement of Telus was the same. For example, to produce:

On Wednesday, March 31, 2010 at 2:00 p.m. (E.S.T.) information from March 30, 2010 at 11:00 a.m. to March 31, 2010 at 11:00 a.m.

[13] Ms. McNish describes in her affidavit what the General Warrant required of Telus. Commencing at 11:00 a.m., one of five Telus security analysts must review records from three databases and then export the records into three Excel documents. The documents must then be combined and sorted in chronological order. Records outside the 24-hour time period must be deleted. The results must then be formatted, password secured and e-mailed by 2:00 p.m.

[14] Ms. McNish states that the General Warrant must, for the requisite time each day, be given priority over the approximately 350 other court orders Telus processes each month.

[15] Ms. McNish notes that, in contrast, Telus has an efficient means of automatically capturing text messages pursuant to an

authorization to intercept private communications. All that is required of Telus is to program a device. This results in all text messages to and from the target being sent directly to the police whose responsibility it is to capture and store the required data.

Criminal Code Provisions

Conventional warrants

[16] By conventional warrants, I mean warrants other than a general warrant or a wiretap authorization. For example:

- (a) section 487 of the *Criminal Code*, which authorizes a justice to grant a search warrant which can include the ability to search a computer system and printout data;
- (b) section 487.012, which allows a judge or justice to order a person to produce data, and prepare documents based on data, in a specified form and within a specified time;
- (c) section 492.2 of the *Criminal Code*, which authorizes a justice to permit the installation of a number recorder on a telephone and the production of records respecting telephone calls made from or to a particular telephone number.

General warrants

[17] Section 487.01 of the *Criminal Code* authorizes a judge to issue a general warrant to use any device or investigative technique or procedure or do anything outlined in the warrant. The authority is subject to certain conditions and exceptions not relevant to this discussion.

[18] In *R. v. Noseworthy* (1997), 33 O.R. (3d) 641, [1997] O.J. No. 1946, 116 C.C.C. (3d) 376 (C.A.), this section was held to be broad enough to authorize prospective warrants.

[19] In Hutchison's *Canadian Search Warrant Manual 2005* (Toronto: Thomson Carswell, 2004), the author refers to the general warrant provision as "a failsafe provision to ensure that almost any investigative technique is available to appropriate state actors".

[20] Section 487.01(1)(c), which is central to a number of the Telus arguments, provides that a general warrant is only available if

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

Authorizations to intercept private communications

[21] The *Criminal Code* provisions respecting the interception of private communications, commonly referred to as wiretap authorizations, were introduced in 1974 by Bill C-176, which was prefaced by the following:

The purposes of this Bill are

- (a) by amendments to the *Criminal Code*, to create offences related to
 - (i) the interception of private communications by the use of any device or apparatus defined to be an electromagnetic, acoustic, mechanical or other device,
 - (ii) the disclosure of private communications intercepted by the use of any such device, and
 - (iii) the possession, sale or purchase of any such device or apparatus or any component thereof the design of which renders it primarily useful for surreptitious interception of private communications;

and to establish rules regarding the admissibility of evidence obtained by the interception of private communications.

[22] Part VI of the Code, titled “Invasion of Privacy”, begins in s. 183 with the following definitions:

“authorization” means an authorization to intercept a private communication given under section 186 or subsection 184.2(3), 184.3(6) or 188(2);

“electro-magnetic, acoustic, mechanical or other device” means any device or apparatus that is used or is capable of being used to intercept a private communication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

“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[.]

[23] Section 185 of the *Criminal Code* provides that an application for an authorization can only be made by designated officials and must be made to a Superior Court Judge. Section 186(1) of the *Criminal Code* provides:

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

- (a) that it would be in the best interests of the administration of justice to do so; and
- (b) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

Inherent Jurisdiction to Review the General Warrant

[24] The parties supplemented their oral submissions with written submissions as to

- (a) the scope of the court's inherent jurisdiction to review the General Warrant; and
- (b) whether it was appropriate for the court to review the documents, now in a sealed packet, reviewed by Thompson J. prior to issuing the General Warrant.

[25] As to the scope of the inherent jurisdiction, Telus characterizes this as the ability to conduct a *de novo* review of the order.

[26] The position of the Crown, from its written submissions responding to Telus, can be summarized as follows:

- (a) The Crown agrees with Telus that "Pursuant to its inherent jurisdiction, this Court has the power to consider new evidence and submissions that the issuing judge did not have the benefit of hearing." The superior court is one of coordinate jurisdiction. Your Honour stands in the same place as Justice Thompson would have stood, had Thompson J. been the judge hearing this application.
- (b) . . . the Crown does not agree with Telus that "The inherent jurisdiction invoked on the Application permits what is effectively a *de novo* review of the Order" or "an examination tantamount to a subfacial review if necessary. To the contrary, the scope of such a review is not limitless." Rather, as the cases relied upon by the Crown clearly show, the court's inherent jurisdiction to review its own process exists to permit the court to remedy or prevent an abuse of process. This is true whether it is the issuing judge who considers the application, or another judge of coordinate jurisdiction. This is also the scope of review that is most consistent with grounds for relief advanced by Telus on this application.

[27] If, as submitted by the Crown, the court's jurisdiction to review the General Warrant is limited, then Telus asserts that it has standing to challenge the General Warrant on the ground that it violates the *Canadian Charter of Rights and Freedoms* right of Telus to be free from unreasonable search and seizure. It, therefore, is only necessary to consider those *Charter* arguments if the court would not otherwise have the jurisdiction to conduct the review or grant the relief sought by Telus.

[28] The position of Telus is that it is open to me to review the sealed packet if I think that would assist but that it is not necessary to do so. Telus cites *R. v. Wilson*, [1983] 2 S.C.R. 594, [1983] S.C.J. No. 88 as authority that supports reviewing the sealed packet. The position of the Crown is that I have no jurisdiction to review the sealed packet.

[29] I have some difficulty understanding and accepting the Crown position to the extent that the Crown argues that my jurisdiction is limited to preventing an abuse of process and that I cannot and should not review the sealed packet. Telus originally sought to return this application before Thompson J., the judge who issued the General Warrant. If Thompson J. heard the application, I do not see how his jurisdiction or discretion would be limited to remedying an abuse of process. If the application was returned before Thompson J., and if the Crown is correct, Thompson J. could be in the position of ruling:

If I had known when I first considered the General Warrant what I now know, I would not have issued it. Nevertheless, having issued it I cannot vary or rescind General Warrant unless to let it stand would amount to abuse of process.

[30] In a similar vein, if the matter had returned before Thompson J., he would know what was in the sealed packet and no doubt factor that into his consideration of whether the issuance of the General Warrant was in the best interests of the administration of justice. I do not see why Telus or the court itself should be in a different position by reason only that the matter has not been returned before the issuing judge.

[31] While I raise these points, I conclude that nothing turns on them. The parties agree that the principal Telus argument, that the General Warrant constitutes an interception of private communications, can and should be decided. The secondary Telus argument is that it was not in the best interests of the administration of justice for the General Warrant to issue. Telus brings this as a test case and is interested in the general principle. The focus of the Telus argument and evidence was on the impact issuing warrants of this type would have on its business. The Telus argument is that this form of search warrant is, as a matter of a general principle, not in the best interests of the administration of justice. To review the sealed packet and to decide the application on the particular facts of this case would do little to establish the general principle contended for by Telus.

[32] I, therefore, did not review the sealed packet. I also need not consider Telus' *Charter* arguments as I am satisfied that my

inherent jurisdiction provides authority to consider all of the arguments and grant the relief sought by Telus.

Does the General Warrant Require Telus to Intercept Private Communications

(i) *The position of Telus*

[33] As discussed, a general warrant is not available if any other statutory provision provides for the type of order sought. Telus contends that the General Warrant purports to authorize the interception of a private communication. As such, a Part VI wiretap authorization was required. Accordingly, a general warrant cannot be issued.

[34] Telus submits the General Warrant authorizes an “interception” of the text messages, given that some text messages will be turned over to the police before they are delivered to and read by the recipient. This is a consequence of the delay that may result due to the recipient not having the phone turned on or not reviewing text messages as received.

[35] Telus argues that there is no requirement that an interception be simultaneous with the transmission of the private communication. This receives some support from U.S. authorities which distinguish between whether a communication is acquired during the progress or course of transmission, in which case an interception has occurred, as opposed to being acquired after the transmission.

[36] Telus cites *United States v. Councilman*, 418 F.3d 67, 2005 U.S. App. LEXIS 16803 (1st Cir. 2005), at 85 F.3d (en banc), for the proposition that messages acquired while in “transient storage that is intrinsic to the communication process” are considered intercepted under the U.S. *Federal Wiretap Act*, 18 U.S.C., c. 119.

[37] Telus concedes that the “case law has generally developed such that in order to qualify as an interception under Part VI, use of some sort of device, as defined in s. 183 is required”. Telus, however, submits that its own computer systems and databases fall within the definition of a “device”.

[38] As to how the police could and should have proceeded, Telus states in its reply factum that

9. . . . the police could serve one production [order] on Telus after the last date in the General Warrant.

(ii) *The position of the Crown*

[39] The Crown submits that, based on the analysis in *R. v. McQueen*, [1975] A.J. No. 342, 25 C.C.C. (2d) 262 (C.A.), an

interception involves an element of “interference between the place of origination and the place of destination of the communication” (para. 7).

[40] Further, the Crown submits on the authority of *R. v. Giles*, [2007] B.C.J. No. 2918, 2007 BCSC 1147, which involved the retrieval of e-mail communications from a Blackberry, that the fact that the General Warrant requires Telus to produce stored data does not constitute an interception. In *Giles*, the court held [at para. 34] that the retrieval did not constitute an interception because “[t]here is a fundamental difference between surreptitiously intercepting and recording messages and simply searching stored messages . . .”. The court confirmed [at para. 45] that an interception “requires that a communication be passing from a source to a destination”. The defining feature for the court in *Giles* was the stored nature of the data.

[41] The Crown submits that an “interception” requires that there be a “contemporaneous diversion of a private communication while it is in transit”.

[42] The Crown also relies upon *Giles* and *McQueen* for the proposition that the use of a “device” is a necessary component of an interception of private communications. Telus, for its own purposes, routinely copies all text messages into databases. As such, no device is involved and there is no state-compelled action constituting an interference with the communication.

(iii) *Analysis and conclusion*

[43] I conclude that the General Warrant does not purport to authorize the interception of private communications for the following reasons:

- (a) giving the word “intercept” its ordinary meaning, it requires a real-time capture of otherwise transient communications; and
- (b) the litmus test to identify an interception submitted by Telus, being whether a sent message has in fact been delivered, is illogical and impractical.

[44] The messaging is clearly a form of private communication as defined in s. 183 of the *Criminal Code*. The real issue is whether the General Warrant purports to authorize the “interception” of a private communication.

[45] The *Criminal Code* provisions respecting the interception of private communications were enacted in 1974, long before text messages could even be imagined. It remains that, if properly

interpreted, these *Criminal Code* provisions capture the process required by the General Warrant then the General Warrant is invalid. The plain meaning of the provisions cannot, however, be disregarded or tortured in aid of adapting the law to modern technology.

[46] First, the meaning of an “intercept”. Telus submits (citing *Application under s. 83.28 of the Criminal Code (Re)*, [2004] 2 S.C.R. 248, [2004] S.C.J. No. 40, at para. 34), and I agree, that the relevant provisions of the Code should be read

... in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament: E.A. Driedger, *Construction of Statutes* (2nd ed. 1983), at p. 87.

[47] The *Canadian Oxford Dictionary* (2nd ed.) provides as the first definition (stated to be the most current and important definition) of “intercept” the following:

Seize, catch or stop (a person, message, vehicle, ball, puck, etc.) going from one place to another.

[48] This definition is consistent with *McQueen* [at para. 7], which, as set out above, defined an interception as involving an “interference between the place of origination and the place of destination of the communication”.

[49] The General Warrant does not in any sense seize, catch, stop or interfere with the progress of text messages from sender to receiver. In fact, the General Warrant is not even directed to text messages in progress. The General Warrant is specifically directed to text messages “stored on [Telus’] computer database”. As noted, Telus stores all messages in its computer database for at least 30 days.

[50] Telus cited *United States v. Councilman*, which held [at 79 F.3d] that messages acquired while in “transient electronic storage that is intrinsic to the communication process” are regarded as intercepted for the purpose of the U.S. *Wiretap Act*. I need not decide whether that interpretation is correct under Canadian law because it is quite clear that messages stored for at least 30 days are not “in transient storage intrinsic to the communication process”.

[51] While that is sufficient to dispose of this application, I will comment briefly on the submissions directed to whether Telus has, in accessing the text messages, utilized a “device”.

[52] Section 184(1) of the *Criminal Code* makes it an offence to intercept a private communication by means of “any electromagnetic, acoustic, mechanical or other device”. Section 184(2) provides, however, that subsection (1) does not apply to a number of

situations, including a telephone service provider in the course of random monitoring necessary for quality control.

[53] As stated in *Sullivan and Driedger on the Construction of Statutes*, 4th ed. (Markham, Ont.: Butterworths, 2002), it is a fundamental principle of statutory interpretation that

... every word and provision found in a statute is supposed to have a meaning and a function. For this reason courts should avoid, as much as possible, adopting interpretations that would render any portion of a statute meaningless or pointless or redundant.

[54] Applying this principle to the interpretation of s. 184, I conclude that the s. 184(2) exceptions are required and have meaning. It follows that, but for the s. 184(2) exceptions, a telephone operator who listened to a conversation would commit an offence. By listening in, the operator would be seizing or catching the private communication in the sense of becoming privy to the content as the parties communicated back and forth.

[55] On this scenario, if one accepts that an offence is committed absent an applicable exception, it is implicit that the telephone operator commits the offence simply by utilizing the existing infrastructure and technology used to carry on the business of the telephone service provider.

[56] If, therefore, the General Warrant had purported to authorize the interception of a private communication, the fact that Telus was able to intercept the communication utilizing its existing infrastructure and technology would not change the fact that the interception was unlawful. In other words, Telus' own computer systems and databases fall within the definition of "device".

[57] Lastly, I address the Telus argument that due to the possibility of a time lag between transmission and receipt of a text message (for example, the recipients' cellphone is not turned on or checked), the General Warrant will result in the interception of some private communications.

[58] It is noteworthy that Telus does not take issue with the right of the Crown to obtain a production order for all text messages sent or received by the subscribers in a prior period. Telus submits that, for example, a production order on April 17, 2010 requiring production of all text messages sent or received during the period March 30-April 16, 2010 is lawful.

[59] Such a production order would, however, also likely result in text messages sent but not yet received being produced to the police. Certain messages that are sent are never received because Telus ceases its efforts to deliver after five days although it stores the message for 30-45 days. Further, to the extent that text messages come from or are sent outside the Telus network,

Telus lacks the means to determine when a text message has been received.

[60] Thus, the form of production order that Telus does not object to, one made at the end of a defined period, runs the same risk of producing sent but not received messages as the General Warrant which Telus does object to. In my opinion, therefore, the question of whether a text message has actually been received cannot be determinative. This standard would be illogical and impractical.

[61] Telus has an arguable point that, as a matter of policy, text messages merit different treatment than traditional business records. It is, however, Parliament, not the court, that is capable of carefully considering the extent to which text messages are analogous to traditional private communications such as a telephone call or conversation, the significance that should be attached to routine storage of text messages and, consequently, the legal requirements which should be applicable.

[62] To take one example, the *Criminal Code* imposes a significant hurdle to the authorities in seeking to intercept private communications. The evidence must establish that other investigative procedures have been tried and have failed or are unlikely to succeed or the urgency is such that the authorization should be granted. Parliament is in the best position to balance the competing interests and determine whether this hurdle should be placed in the way of the authorities seeking access to stored text messages.

Were the Police Obligated to Obtain Conventional Warrants Instead of a General Warrant

[63] As discussed, s. 487.01(1)(c) of the *Criminal Code* provides that a general warrant is only available if there is no other provision, in a federal statute, that would permit the technique, procedure or device.

[64] The position of Telus is that

- (a) the text messages for dates preceding the issuance of the General Warrant could have been obtained by a production order or search warrant. (As noted, the Crown agrees and I will not address this further);
- (b) the future text messages could have been obtained under a Part VI authorization; and
- (c) the subscriber information could have been obtained by a warrant for a dial number recorder and an order for telephone records under s. 492.2(1) and (2) of the Code.

[65] In *R. v. Noseworthy*, *supra*, the court found that s. 487.01 of the *Criminal Code* authorizes [a] prospective search warrant. In that case, the anticipation was that the items to be seized would be at a particular place later on the day the warrant was issued.

[66] In Hutchison's *Canadian Search Warrant Manual 2005*, the author, referring to *R. v. Brooks*, [2003] O.J. No. 3757, 176 O.A.C. 337 (C.A.), stated:

In *Brooks*, the Court of Appeal for Ontario added an important gloss on *Noseworthy*. Anticipatory warrants that “pre-preauthorize” a technique that might otherwise be available do not meet the requirement that no other provision be available, unless the facts of the case make the other conventional warrant impractical. In other words, if a conventional warrant is legally available to achieve the same investigative objective (e.g., seizure of a particular item) and is practicable in the circumstances of the particular case, then that conventional warrant should be pursued rather than s. 487.01 anticipatory general warrant. The anticipatory warrant in *Noseworthy* was justified by the fact that it would not be realistic to return the material and then apply for a warrant to re seize — the only realistic option was an anticipatory warrant.

[67] The Crown relies upon *R. v. Ha* (2009), 96 O.R. (3d) 751, [2009] O.J. No. 1693, 2009 ONCA 340 for the proposition that the “no other provision” test is not about whether the evidence could be obtained by other warrants, but whether other provisions would permit the particular technique or procedure sought to be employed in a general warrant.

[68] The Crown quoted from *R. v. Ha* as follows [at para. 43]:

The focus in the s. 487.01(1)(c) analysis is not on whether there are other investigative techniques that might accomplish the purported investigative purposes or goals of the police; rather, the focus is on the particular investigative technique or procedure that the police seek to utilize and whether it can properly be authorized by another provision in the Code or any other federal statute. In this case, the police sought to obtain authorization to conduct an unlimited number of covert entries and searches on private property over a two-month period. Except for s. 487.01 of the Code, there is “no other provision in . . . any other Act of Parliament” that could potentially accomplish this goal.

[69] Telus takes the position that the police could and should have waited until the end of the 14-day period covered by the General Warrant and then applied for a conventional warrant. I know of no authority which would require the police to wait as opposed to apply periodically for production as they see fit.

[70] The police, therefore, could have gone to a justice of the peace every day for the 14 days covered by the General Warrant and obtained the same records using conventional warrants. There are obvious drawbacks to this approach:

- (a) 14 applications as opposed to one application;

- (b) the probable need for the involvement of more than one justice of the peace;
- (c) the possibility of inconsistent approaches by different justices of the peace; and
- (d) inconvenience to the person to whom the warrant is directed in receiving a daily warrant requiring prompt response.

[71] The Court of Appeal in *Noseworthy* and *Brooks* emphasized that s. 487.01 should be given an expansive interpretation to ensure its ability to serve as a flexible and effective investigative tool.

[72] It is common ground that Telus is required to produce the requested information. The point of contention is whether production should be as a result of a general warrant issued by a judge or a series of conventional warrants issued by a justice of the peace.

[73] I, therefore, also look at this from the perspective of a person, such as Telus, to whom the warrant is directed. This person is naturally concerned about the extent to which compliance with this type of general warrant will intrude on their affairs and interests and impose cost and inconvenience.

[74] The legitimate concerns of such a person are more likely to be addressed by a judge able to consider the full extent of the investigative technique proposed by the police as opposed to multiple justices of the peace considering day-by-day requests.

[75] To paraphrase the reasons in *Ha*, the investigative technique or procedure of prospective and daily production of text messages cannot be authorized under any other statutory provision. As such, a general warrant is available.

[76] Further, given the recognized objective that general warrants serve as a flexible and effective investigative tool, I agree with the interpretation of *Brooks* suggested by Mr. Hutchison. A general warrant is available if the use of a conventional warrant would be impractical in the circumstances. For the reasons discussed, I am satisfied it would have been impractical for the police to obtain a daily warrant to achieve the investigative objective of obtaining stored text messages for daily review.

Was it in the Best Interests of the Administration of Justice for the General Warrant to Issue

[77] Section 487.01 provides as a precondition that it is “in the best interests of the administration of justice” for a general warrant to issue.

[78] If the General Warrant purported to authorize the interception of private communications, I would have set it aside on that basis. My consideration of the best interests of the administration of justice proceeds on the basis, as I have decided, that the *Criminal Code* did not require the police to obtain a Part VI wiretap authorization to obtain the text messages from Telus.

[79] Telus nevertheless submits that the General Warrant should be set aside on the basis that its issuance was not in the best interests of the administration of justice. Specifically, Telus submits that given the high expectation of privacy in text messages, the court should require the police to obtain a Part VI authorization. In support of this conclusion, Telus also notes that the “manual capturing process” to comply with the General Warrant is not as reliable as the “automatic wiretap process” by which all text messages can simply be diverted for review by the police.

[80] As previously discussed, Parliament has laid down the requirements to obtain various types of warrants and authorizations. I have decided that to obtain these text messages, a Part VI authorization (which requires evidence of investigative necessity) is not required. That is the legislative scheme. In my opinion, it is not open to the court to decide on public policy grounds that the legislative scheme is inappropriate and, under the guise of what is in the best interests of the administration of justice, effectively expand the ambit of Part VI of the *Criminal Code*.

[81] I appreciate that Telus has business concerns if similar general warrants become common. Telus has indicated a particular concern about the tight turnaround time under the General Warrant and the fact that computer system limitations may prevent perfect compliance with the General Warrant as some messages in the relevant time frame may not be caught by a database search.

[82] Telus has raised these concerns in the material filed on this application and to some extent they are reflected in these reasons. It is open to Telus to summarize its concerns in a letter to the Crown and/or police services with a request that a copy of the letter be provided to any judge hearing an *ex parte* application of this nature.

[83] While the issue is not before me, and I make no ruling, it appears to me Telus has an argument that the obligation on any party making an *ex parte* application to make full disclosure of relevant facts would extend to disclosing the known concerns and position of Telus.

[84] In this regard, Molloy J. stated in *R. v. Alvarez*, [2009] O.J. No. 3825, 2009 CarswellOnt 5448 (S.C.J.), at para. 18:

Because the application for a wiretap authorization is made by the Crown on an *ex parte* basis, there is a duty to make full, fair and frank disclosure, not just of the material upon which the Crown relies, but also of any facts that that would support the position of anyone opposed to the authorization being granted: *R. v. Araujo*, [2000] 2 S.C.R. 992 (S.C.C.) at paras. 46-47.

[85] Finally, s. 487.01(1) provides that if the statutory criteria are met, the judge “may” issue a general warrant. It would be open to the judge to conclude, on the evidence filed, that there was no practical advantage to a general warrant as opposed to a conventional warrant. It would also be open to the judge to factor into the exercise of discretion the cost and inconvenience to the person to whom the general warrant was directed.

[86] To a considerable extent, the cost and inconvenience would, as a matter of common sense, be evident. Further, the police may well be required to apprise the judge of particular concerns, of the nature cited by Telus, to the extent they are known to the police.

[87] The fact that significant costs will necessarily be incurred in assisting law enforcement agencies does, however, to a great extent go with the territory. In *R. v. Tele-Mobile Co.* [aka Telus Mobility] (2008), 92 O.R. (3d) 478, [2008] 1 S.C.R. 305, [2008] S.C.J. No. 12, Telus took the position that the burden of compliance with production orders, issued under s. 487.012(1) of the *Criminal Code*, would be unreasonable unless Telus was compensated for the cost of retrieving archived data. Telus estimated the annual cost of complying with production orders would be \$662,000.

[88] I think it fair to say the Supreme Court of Canada was unimpressed with Telus’ arguments based upon financial impact. As Abella J. stated for the court [at para. 60]:

I accept Telus’ concern that because of the nature of its business, it will necessarily be the object of repeated production orders but, as an American court observed in connection with banks, another entity from whom requests for information are routinely sought, such requests are neither unanticipated nor aberrational:

Any further expenses incurred in connection with this investigation and examination of these records, such as the salary of employees that may be necessarily assigned to this project, are expenses to be borne by the bank. . . . They are reasonably incident to the bank’s normal operations, and they are reasonable expenses that the bank can be and should be prepared to sustain when it opens and operates as a bank, knowing full well that some of its depositors will from time to time get investigated by the Internal Revenue Service.

(*U.S. v. Jones*, 351 F. Supp. 132 (M.D. Ala. 1972), per Johnson C.J., at p. 134)

Conclusion

[89] The Crown conceded, and I order, that the General Warrant should be rescinded to the extent that it requires the production of text messages in existence prior to the issuance of the General Warrant. The Telus application is otherwise dismissed.

Application granted in part.

Carnell et al. v. Aviva Canada et al.

[Indexed as: Carnell v. Aviva Canada]

2010 ONSC 6359

*Superior Court of Justice, Mullins J. December 2, 2010**

Insurance — Automobile insurance — Exclusions — Insured losing control of his vehicle while participating in driver education event at racetrack — Event designed to teach participants to drive at higher speeds in controlled environment — Racing and timing devices prohibited — Insured not using automobile in race or speed test at time of accident.

The insured owned a modified Porsche. He was participating in a driver education event operated by the Porsche Club of America at a racetrack when he lost control and rolled the vehicle. Section 4.2 of *Statutory Conditions — Automobile Insurance*, O. Reg. 777/93 prohibits use of an automobile in a race or speed test. The insured applied for a declaration that he did not fall within that exclusion at the time of the accident.

Held, the application should be granted.

The driver education event was designed to teach participants to drive at higher speeds in controlled environments. Racing and timing devices were not allowed, and there was no start or finish line. A race is a test between rivals. Factors common to a race are as follows: vehicles operating at high speed, in close proximity, over a fixed distance; abrupt lane changes; blocking; bold manoeuvres; jockeying for position; and high-risk passing. At the time of the accident, the insured was not engaged in a competitive activity that met the definition of a race, nor was he seeking to test the speed of his vehicle.

Cases referred to

Blackstock v. Insurance Corp. of British Columbia, [1982] B.C.J. No. 1480, 138 D.L.R. (3d) 563, 38 B.C.L.R. 339, 15 A.C.W.S. (2d) 387 (S.C.); *Gore Mutual Insurance Co. v. Rossignoli*, [1964] 2 O.R. 274, [1964] O.J. No. 758, 45 D.L.R. (2d) 216 (C.A.); *McGuinness v. Canadian General Insurance Co.*, [1976] B.C.J. No. 82, 66

* This judgment was recently brought to the attention of the editors.