R v Telus Communications Co (2013): Police Need Wiretap Warrant to Seize Text Messages

Introduction

On March 27, 2013, the Supreme Court of Canada ruled[1] that the interception of text messages requires wiretap authorization[2] found under Part VI of the *Criminal Code*.[3] Part VI of the *Criminal Code* protects private communications, such as phone calls, from being intercepted by the police.[4] If the police require access to private communications for investigation purposes, a judge must issue a wiretap warrant.[5] The*R v Telus* decision now requires the police to apply for a wiretap warrant if they wish to seize text messages.[6] The scope of the wiretap authorization was extended to include text messages in order to protect people's right against unreasonable search and seizure guaranteed under section 8 of the *Canadian Charter of Rights and Freedoms* (*Charter*).[7]

Facts

Telus' Transmission Process

When Telus subscribers send a text message, the following process occurs: (1) the text message is sent to the nearest cell tower, (2) from the cell tower it is sent toTelus' transmission tower, (3) from the transmission tower is it sent to the cell tower closest to the recipient, and (4) finally it is sent from the cell tower to the recipient's phone.[8] When a text message is sent to the Telus transmission tower, the text message is electronically copied to a computer database and stored for up to 30 days.[9] Telus is the only major telecommunications service provider that stores electronic copies of its subscribers' text messages.[10] Telus' unique transmission process results in text messages being copied and stored on a computer database before the recipient has received the text message.[11]

The General Warrant

On March 27, 2010 Owen Sound Police Service obtained a general warrant under section 487.01 of the*Criminal Code*.[12] The warrant named two Telus subscribers, and stated that the police needed access to text messages sent and received by these two individuals. Telus was to produce the text messages according to the following schedule:

1. Telus was to provide copies of all the text messages that were currently stored on the computer database immediately.

2. On March 30, 2010, Telus was to provide copies of the messages that were stored on the database from March 18 to March 30.

3. On a daily basis, from March 31 until April 16, Telus was to provide the text messages sent and received within the last 24 hours. Only these text messages were at issue in this case.[13]

Telus argued that the general warrant was invalid because the police failed to satisfy all of the requirements listed under section 487.01 of the *Criminal Code*.[14]

General Warrants vs. Wiretap Warrants

A general warrant can be issued by a judge under section 487.01 of the *Criminal Code*[15] if there are no other provisions in the *Criminal Code* "that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done."[16]

Part VI of the *Criminal Code* protects private communications from being intercepted.[17] Accordingly, section 184(1) of the *Criminal Code* makes it a criminal offence to wilfully intercept a private communication.[18] If the police need to intercept a private communication for investigation purposes, they must apply for a wiretap warrant.[19]

If retrieving electronic copies of text messages stored on a computer database counts as "intercepting a private communication," then the general warrant was invalid because there was another *Criminal Code*provision available to the police, namely a wiretap warrant.[20]

Procedural History

In 2011, Telus applied to the Ontario Superior Court of Justice to have the warrant declared invalid because it was improperly obtained.[21] Telus' application was dismissed because the trial judge ruled that no other provision was available to the police.[22] Specifically, the trial judge ruled that the "no other provision" requirement referred to a technique or procedure, not whether the evidence could be obtained by another warrant using a different technique.[23]

Telus appealed the Ontario Superior Court of Justice decision to the Supreme Court of Canada. Telus again argued that there was another provision available to the investigating officers and as a result, the general warrant was invalid.

Issues

The Supreme Court of Canada considered the following issues:

1. Was the general warrant valid?

2. If the general warrant was invalid, what is the legal remedy?

Decision

The majority of justices on the Supreme Court of Canada ruled that the general warrant was

invalid because the investigating officers required wiretap authorization to seize text messages stored on a computer database.[24] As a result, the Court allowed Telus' appeal and declared that the general warrant was void.[25]

Court's Analysis

Issue 1: Was the General Warrant Valid?

Section 8 of the *Charter* states: "Everyone has the right to be secure against unreasonable search or seizure."[26] As a general rule, for a search or seizure to be valid and not violate section 8 of the *Charter*, the police must have received judicial authorization before the search or seizure occurred.[27] A general warrant and a wiretap warrant are examples of judicial authorization. In *R v Telus*, the Supreme Court of Canada had to determine which type of warrant was required to seize text messages stored on a computer database.[28]

The majority of justices on the Supreme Court of Canada determined that the general warrant was invalid, but the justices had different reasons for coming to this conclusion. Justice Abella (writing for herself and Justices LeBel and Fish) determined that seizing text messages constituted an interception of private communications and therefore, the police needed a wiretap warrant.[29] Justice Moldaver (writing for himself and Justice Karakatsanis) ruled that the general warrant was invalid because the police had access to a different type of authorization (wiretap warrant).[30]

Justice Abella's Judgment

Justice Abella's analysis focused on the definition of "interception" in section 183 of the *Criminal Code* and the purpose of Part VI of the *Criminal Code*.[31] When interpreting the *Criminal Code* in light of recent technological advancements, Justice Abella noted that courts must remain aware of people's privacy rights protected by section 8 of the *Charter*.[32] Justice Abella determined that people have the same expectation of privacy in their text messages as in their phone calls.[33] The primary difference between the two modes of conversation, text messages and phone calls, is the transmission process.[34] As a result, Justice Abella defined "interception" as referring to any communication that would convey its substance or meaning.[35] This broad definition is necessary because Parliament intended Part VI of the *Criminal Code*to protect private communications regardless of the transmission process.[36]

Justice Abella, therefore, determined that the retrieval of text messages was an interception of private communications.[37] To intercept private communications for investigation purposes, the police must receive a wiretap warrant.[38] Because a wiretap warrant was available to the police, Justice Abella ruled that the general warrant was invalid.[39]

Justice Moldaver's Judgment

Justice Moldaver's analysis focused on the "no other provision" requirement in section 487.01(1)(*c*) of the*Criminal Code*.[40] The "no other provision" requirement means that if another type of warrant was available to seize text messages stored on a computer

database, then the general warrant was invalid. Justice Moldaver noted that the police could have obtained a wiretap warrant but chose to pursue a general warrant instead.[41] Justice Moldaver attributed this decision to the fact that it is easier to get a general warrant than a wiretap warrant.[42] The police must satisfy additional requirements before a wiretap warrant is issued, such as identifying the target of the interception and providing the target with notice that his or her private communications will be intercepted.[43] These additional safeguards are in place to protect people's private communications from undue state interference.[44] Justice Moldaver stated that the general warrant should not be used as a way to avoid these safeguards.[45] Overall, the police could have obtained a wiretap warrant and therefore, the general warrant is invalid.[46]

Justice Cromwell's Dissent

Justice Cromwell (writing for himself and Chief Justice McLachlin) determined that the general warrant was valid because the police did not intercept the text messages and no other type of warrant was available.[47]First, Justice Cromwell disagreed with Justice Abella's definition of "interception" because it failed to draw a distinction between interception and disclosure.[48] Justice Cromwell stated that Telus intercepted the text messages and then disclosed them to the police.[49] Because the police did not intercept the text messages, Part VI of the *Criminal Code* (wiretap authorization) did not apply in this case.[50]

Second, Justice Cromwell interpreted the "no other provision" requirement in section 487.01(1)(*c*) of the*Criminal Code* as referring to a warrant that would authorize the same technique, not a different technique that would produce the same results.[51] A wiretap warrant would achieve the same results as the general warrant, but the investigation techniques are different. For instance, the general warrant would provide the police with copies of the text messages. The wiretap warrant, however, would require the police to obtain telephone records, secure a listening post to receive the messages, and organize police officers to process and sort the incoming data.[52] As a result, the "no other provision" requirement was satisfied and the general warrant was valid.[53]

Issue 2: If the general warrant was invalid, what is the legal remedy?

The majority of the justices on the Supreme Court of Canada (Justices Abella, LeBel, Fish, Moldaver, and Karakatsanis) ruled that the general warrant was improperly obtained because there was another provision in the *Criminal Code*, specifically the wiretap authorization.[54] Since the general warrant was improperly obtained, Telus' appeal was allowed and the general warrant was void.[55]

Significance of the Ruling

R v Telus requires the police to obtain a wiretap warrant before they seize text messages stored on a computer database.[56] Because of this Supreme Court of Canada decision, both phone calls and text messages are protected from undue state interference. The transmission process is markedly different for phone calls and text messages; however,

people have a reasonable expectation of privacy in both modes of communication. As a result, both forms of private communication are protected from unreasonable search and seizure, a constitutionally guaranteed right under section 8 of the *Charter*.[57]

R v Telus is just one example of several cases that have recently come before the courts dealing with changing technology and people's privacy rights.[58] This recent trend may prompt the Federal Government to amend certain search and seizure provisions in the *Criminal Code*.[59] If the *Criminal Code*[60] was amended to more accurately reflect search and seizure procedures related to modern technology, there would be greater clarity for judges, investigating officers, and the general public.

[1] *R v Telus Communications Co*, 2013 SCC 16 <http://scc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/en/item/12936/index.do>.

[2] Wiretapping is a form of electronic surveillance enabling investigators to monitor private telephone communications. Wiretap authorization is a form of search warrant that enables investigators to lawfully monitor private telephone communications.

[3] *Criminal Code*, RSC 1985, c C-46 ss 183-96 <http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-46/latest/rsc-1985-c-c-46.html>.

[4] *Ibid*.

[5] *Ibid*, s 185.

[6] *Telus*, *supra* note 1.

[7] *Canadian Charter of Rights and Freedoms*, s 8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 ("[e]veryone has the right to be secure against unreasonable search or seizure," s 8) <http://laws-lois.justice.gc.ca/eng/const/page-15.html>.

[8] *Telus*, *supra* note 1 at para 6.

[9] *Ibid* at para 7.

[10] Telus copies and stores text messages on a computer database to assist in troubleshooting and managing customer complaints.

[11] *Telus*, *supra* note 1 at para 7.

[12] *Code*, *supra* note 3, s 487.01.

[13] *Telus*, *supra* note 1 at paras 8-9.

[14] *Code*, *supra* note 3, s 487.01; *Telus*, *supra* note 1 at para 10.

[15] *Code*, *supra* note 3, ss 487.01, 487.01(1)(*c*).

[16] *Ibid*.

[17] *Ibid*, ss 183-96.

[18] *Ibid*, s 184(1).

[19] *Ibid*, s 185.

[20] *Ibid*, ss 183, 185, 487.01.

[21] *R v Telus Communications Co*, 2011 ONSC 1143 <http://www.canlii.org/en/on/onsc/doc/2011/2011onsc1143/2011onsc1143.html>.

[22] *Ibid* at para 75.

[23] *Ibid* at paras 67-75.

[24] *Telus*, *supra* note 1 at paras 45, 106.

[25] *Ibid* at paras 46, 108.

[26] *Charter*, *supra* note 7.

[27] *Hunter et al v Southam Inc*, [1984] 2 SCR 145 <http://csc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/en/item/5274/index.do>.

[28] *Telus*, *supra* note 1.

[29] *Ibid* at paras 43-46.

[30] *Ibid* at para 106.

[31] *Code*, *supra* note 3.

[32] *Telus*, *supra* note 1 at para 33; *Code*, *supra* note 3; *Charter*, *supra* note 7.

[33] *Telus*, *supra* note 1 at para 1.

[34] *Ibid*.

[35] *Ibid* at para 25.

[36] *Ibid* at para 33; *Code*, *supra* note 3.

[37] *Telus*, *supra* note 1 at para 35.

[38] *Code*, *supra* note 3.

[39] *Telus*, *supra* note 1 at para 45.

[40] *Code*, *supra* note 3, s 487.01(1)(c).

[41] *Telus*, *supra* note 1 at para 49.

[42] *Ibid* at paras 73, 74.

[43] *Ibid* at para 73.

[44] *Ibid* at para 78.

[45] *Ibid* at para 76.

[46] *Ibid* at paras 106, 108.

[47] *Ibid* at paras 109, 130.

[48] *Ibid* at para 145.

[49] *Ibid* at paras 149-50.

[50] *Ibid* at para 159; *Code*, *supra* note 3.

[51] *Ibid*, s 487.01(1)(c); *Telus*, *supra* note 1 at para 164.

[52] *Ibid* at para 179.

[53] *Ibid* at paras 195-96.

[54] *Ibid* at paras 45, 106.

[55] *Ibid* at paras 46, 108.

[56] *Ibid*.

[57] *Charter*, *supra* note 7.

[58] *Telus*, *supra* note 1; *R v Cole*, 2012 SCC 53, [2012] 3 SCR 4 <http://scc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/en/12615/1/document.do>; *R v Fearon*, 2013 ONCA 106 <http://canlii.ca/en/on/onca/doc/2013/2013onca106/2013onca106.html>.

[59] *Code*, *supra* note 3.

[60] *Ibid*.