SCC File No.: 37194

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO)

B E T W E E N:

TRISTAN 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, DIRECTEUR DES POURSUITES CRIMINELLES ET PENALES DU QUEBEC, CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO, CANADIAN CIVIL LIBERTIES ASSOCIATION, SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Interveners

FACTUM OF THE INTERVENER BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

(pursuant to Rules 37 and 42 of the *Rules of the Supreme Court of Canada*)

STOCKWOODS LLP
TD North Tower
77 King Street West, Suite 4130
Toronto, Ontario M5K 1H1

Gerald Chan / Nader R. Hasan
Tel: (416) 593-1617
Fax: (416) 593-9345
Email: GeraldC@stockwoods.ca
Email: NaderH@stockwoods.ca

Counsel for the Intervener, British Columbia Civil Liberties Association

POWER LAW
130 Albert Street
Suite 1103
Ottawa, Ontario K1P 5G4

David Taylor
Tel: (613) 702-5563
Fax: 1 (888) 604-2227
Email: dtaylor@powerlaw.ca

Ottawa Agent for the Intervener, British Columbia Civil Liberties Association

ORIGINAL TO:

SUPREME COURT OF CANADA
The Registrar
301 Wellington Street
Ottawa, Ontario
K1A 0J1

COPIES TO:

FASKEN MARTINEAU
55 Metcalfe Street, Suite 1300
Ottawa, Ontario K1P 6L5

Patrick McCann
Peter Mantas
Ewan Lyttle
Tel: (613) 696-6906
Fax: (613) 230-6423
Email: pmccann@fasken.com

Counsel for the Appellant,
Tristin Jones

SUPREME ADVOCACY LLP
100- 340 Gilmour Street
Ottawa, Ontario K2P 0R3

Marie-France Major
Tel: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Ottawa Agent for the Appellant,
Tristin Jones

ATTORNEY GENERAL OF ONTARIO
720 Bay Street, 10th Floor
Toronto, Ontario M7A 2S9

Randy Schwartz
Tel: (416) 326-4586
Fax: (416) 326-4656
Email: randy.schwartz@ontario.ca

Counsel for the Respondent,
Her Majesty the Queen in Right of Ontario

BURKE-ROBERTSON
441 MacLaren Street, Suite 200
Ottawa, Ontario K2P 2H3

Robert E. Houston, Q.C.
Tel: (613) 236-9665
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Ottawa Agent for the Respondent,
Her Majesty the Queen in Right of Ontario

AND TO:

PUBLIC PROSECUTION SERVICE OF CANADA
130 King Street West
Suite 3400, Box 36
Toronto, Ontario M5X 1K6

Nicholas E. Devlin
Tel: (416) 952-6213
Fax: (416) 952-2116
Email: nick.devlin@ppsc-sppc.gc.ca

**Counsel for the Intervener,
Her Majesty the Queen in Right of Canada**

DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA
160 Elgin Street, 12th Floor
Ottawa, Ontario K1A 0H8

François Lacasse
Tel: (613) 957-4770
Fax: (613) 941-7865
Email: francois.lacasse@ppsc-sppc.gc.ca

**Ottawa Agent for the Intervener,
Her Majesty the Queen in Right of Canada**

ATTORNEY GENERAL OF BRITISH COLUMBIA
3rd Floor - 940 Blanshard Street
Victoria, British Columbia V8W 3E6

Daniel M. Scanlan
Tel: (250) 387-0284
Fax: (250) 387-4262
Email: daniel.scanlan@gov.bc.ca

**Counsel for the Intervener,
Attorney General of British Columbia**

BURKE-ROBERTSON
441 MacLaren Street, Suite 200
Ottawa, Ontario K2P 2H3

Robert E. Houston, Q.C.
Tel: (613) 236-9665
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

**Ottawa Agent for the Respondent,
Attorney General of British Columbia**

DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC
2050, rue Bleury bureau 6.00
Montréal, Quebec H3A 2J5

Ann Ellefsen-Tremblay
Tel.: (514) 873-6493 Ext.
Fax: (514) 873-6475
ann.ellefsen-tremblay@dpcp.gouv.qc.ca

**Counsel for the Intervener,
Directeur des poursuites criminelles et pénales du Québec**

DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC
17, rue Laurier, Bureau 1.230
Gatineau, Quebec J8X 4C1

Emily K. Moreau
Tel.: (819) 776-8111 Ext. 60412
Fax: (819) 772-3986
Email: emily-k.moreau@dpcp.gouv.qc.ca

**Agent for the Intervener,
Directeur des poursuites criminelles et pénales du Québec**

AND TO:

URSEL PHILLIPS FELLOWS HOPKINSON LLP
555 Richmond Street West, Suite 1200
Toronto, Ontario M5V 3B1

Susan M. Chapman
Naomi Greckol-Herlich
Tel: (416) 969-3061
Fax: (416) 968-0325
Email: schapman@upfhlaw.ca

Counsel for the Intervener, Criminal Lawyers' Association (Ontario)

SUPREME ADVOCACY LLP
100- 340 Gilmour Street
Ottawa, Ontario K2P 0R3

Marie-France Major
Tel: (613) 695-8855 Ext: 102
Fax: (613) 695-8580
Email: mfmajor@supremeadvocacy.ca

Ottawa Agent for the Intervener, Criminal Lawyers' Association (Ontario)

MCCARTHY TÉTRAULT LLP
Toronto Dominion Bank Tower
Box 48, Suite 5300
Toronto, Ontario M5K 1E6

Christine Lonsdale
Charlotte-Anne Malischewski
Tel: (416) 601-8019
Fax: (416) 868-0673
Email: clonsdale@mccarthy.ca

Counsel for the Intervener, Canadian Civil Liberties Assosciation

CONWAY BAXTER WILSON LLP
400 - 411 Roosevelt Avenue
Ottawa, Ontario K2A 3X9

Colin S. Baxter
Tel: (613) 780-2012
Fax: (613) 688-0271
Email: cbaxter@conway.pro

Ottawa Agent for the Intervener, Canadian Civil Liberties Assosciation

PRESSER BARRISTERS
116 Simcoe Street, Suite100
Toronto, Ontario M5H 4E2

Jill R. Presser
Ian R. Kerr
Tel: (416) 586-0330
Fax: (416) 596-2597
Email: presser@presserlaw.ca

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC
University of Ottawa, Faculty of Law
57 Louis Pasteur Street
Ottawa, Ontario K1N 6N5

Tamir Israel
Tel: (613) 562-5800 Ext: 2914
Fax: (613) 562-5417
Email: tisrael@cippic.ca

Ottawa Agent for the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic

TABLE OF CONTENTS

PART I: STATEMENT OF FACTS

1. The British Columbia Civil Liberties Association (the "BCCLA") accepts the facts as set out in the parties' facta and takes no position on disputed facts.

PART II: THE BCCLA'S POSITION ON THE QUESTION IN ISSUE

2. The BCCLA intervenes only on one issue in this appeal: whether a Part VI authorization is required for the police to acquire text messages from a telecommunications provider that already exist at the time the police seek judicial authorization. The BCCLA respectfully submits that the answer is "yes".

3. Canadians are increasingly communicating by text messaging.[1] As one judge put it, "much of our communication that was once exclusively verbal is now by electronic text."[2] In other words, 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.

4. Text messages are often stored in the computers of third party service providers — whether they be telecommunications providers like Telus or technology companies that provide instant, text-based messaging services through "apps" like "WhatsApp".[3] Where the police seek to acquire these text messages from third party service providers, they should be required to meet the same stringent standards that would have applied had the police sought to acquire voice communications through a wiretap (*i.e.*, Part VI of the *Criminal Code*). Technical differences in the mode of communication should not determine the privacy rights of Canadians — especially since this Court has already held that text messages are "private communications" within the meaning of Part VI.

5. Thus, the BCCLA submits that a Part VI authorization should be required whenever the police acquire text messages from a third party service provider that has stored those communications. This approach is rooted in the purpose and text of Part VI (including the expansive definition of "intercept" in s. 183). And contrary to the submissions of the Crown

---

[1] See the BCCLA's factum in the companion appeal, *R. v. Marakah*, SCC File No. 37718.

[2] *R. v. Giles*, [2007] B.C.J. No. 2918 at para. 43 (S.C.).

[3] Matt Puzzo, "WhatsApp Encryption Said to Stymie Wiretap Order", *New York Times*, 12 March 2016.

respondents, this approach would not result in the extension of Part VI to police searches of users' personal devices (*e.g.*, personal computers and cell phones). The latter is distinguishable in light of this Court's decision in *R. v. TELUS Communications Co.* ("*TELUS*").[4]

PART III: STATEMENT OF ARGUMENT

I. "INTERCEPT" SHOULD NOT BE TEMPORALLY LIMITED

6. The question raised in this appeal concerns the scope of Part VI of the *Criminal Code.* This is an issue of statutory interpretation. The words of the statute must be "read in their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament."[5]

7. While Part VI is often thought of as the wiretapping scheme in the *Criminal Code*, it is broader.[6] It applies to the interception of ***all*** private communications. This Court has already held that text messages are "private communications" within the meaning of Part VI.[7] Therefore, the dispute in this appeal concerns the meaning of "intercept".

8. The Crown respondents focus largely on the plain and ordinary meaning of the word "intercept", which they suggest requires that the State actor step between the sender and recipient of a communication,[8] or interfere with the message between the place of origination and place of destination.[9] In other words, they focus on the temporal element of the State act which they say is critical to the question of whether it qualifies as an "intercept". These submissions, however, overlook the scheme and object of Part VI, both of which are discussed in *TELUS.* While not determinative of the issue in this appeal, *TELUS* represents a critical starting point as it is the only case in which this Court has considered the application of Part VI to the interception of text messages.

---

[4] *R. v. TELUS Communications Co.*, [2013] 2 S.C.R. 3 ["*TELUS*"].

[5] *Re Rizzo & Rizzo Shoes Ltd.*, [1998] 1 S.C.R. 27 at para. 21.

[6] *Lyons v. The Queen*, [1984] 2 S.C.R. 633 at 664; *TELUS*, *supra* at para. 24 per Abella J. (S.C.C.).

[7] Indeed, all seven justices who sat in *TELUS* reached this conclusion: see para. 12 per Abella J., para. 67 per Moldaver J., and para. 135 per Cromwell J.

[8] Factum of the the Respondent, Her Majesty the Queen (in right of Ontario), para. 78.

[9] Factum of the the Respondent, Her Majesty the Queen (in right of Ontario), para. 78

9. In *TELUS*, the police had obtained a general warrant under s. 487.01 of the *Criminal Code* that required Telus to produce text messages sent or received within the last 24 hours on a daily basis over a 13-day period, starting three days after the date of the warrant.[10] The plurality opinion of Abella J. found that this investigative technique was an "intercept", and, therefore, an authorization under Part VI was required.[11] The concurring opinion of Moldaver J. concluded that this was the "substantive equivalent" of an "intercept" such that the police could not rely on a less stringent search and seizure provision (*i.e.*, s. 487.01).[12]

10. Both Abella J. and Moldaver J. explicitly limited their opinions to considering the acquisitions of *future* text messages (*i.e.*, those not yet in existence at the time of judicial authorization). The reasoning underlying both opinions, however, goes further. It supports the application of Part VI to the acquisition of text messages already exchanged at the time of judicial authorization.

11. Abella J. started her analysis by noting that "intercept" is a defined term. Section 183 defines "intercept" to include three separate acts, any one of which is sufficient: "listen to", "record", or "acquire".[13] The first two acts do not apply to text communications, which cannot be listened to and are already recorded by the time the State seeks to acquire them (either in the user's own device or in the servers of the service provider). The third act, however, is critical. As Abella J. held in *TELUS*, rather than limit the definition of "intercept" to its "narrow, technical definition", the term "acquire" has the effect of "broaden[ing] the concept of interception."[14] This led her to the conclusion that "(t)here 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."[15] Thus, the Crown respondents' attempt to impose a temporal limitation on the term "intercept" is misguided.

12. The breadth of the language of Part VI mirrors the breadth of its purpose. Part VI represents the high watermark of rights-protecting legislation. Parliament established a stringent

---

[10] *TELUS*, *supra* at para. 9 per Abella J. (S.C.C.).

[11] *TELUS*, *supra* at paras. 37, 43 per Abella J. (S.C.C.).

[12] *TELUS*, *supra* at paras. 49, 97, 106 per Moldaver J. (S.C.C.).

[13] *TELUS*, *supra* at para. 25 per Abella J. (S.C.C.).

[14] *TELUS*, *supra* at para. 35 per Abella J. (S.C.C.).

[15] *TELUS*, *supra* at para. 35 per Abella J. (S.C.C.).

set of requirements that the police must meet before they can access our innermost thoughts and ideas as expressed through our private communications. As Abella J. observed in *TELUS*, the safeguards provided for in Part VI "illuminate Parliament's intention that a higher degree of protection be available for private communications."[16] Contrary to the holding of the court below,[17] Parliament focused on the nature of the information sought (and not on the timing of when it is sought).

13. This is borne out by the legislative history. Part VI of the *Criminal Code* (formerly Part IV) was part of the *Protection of Privacy Act* introduced in Parliament in 1973. During the second reading of the bill in the House of Commons, legislators made the following statements:

- Hon. Otto E. Lang (Minister of Justice): "But in this bill, for the first time at a federal level, the right of privacy is recognized expressly in a protection of privacy act. We are all familiar with the deep felt belief that privacy and individuality are of fundamental importance to our democratic way of life. With the growth of electronic devices which make it possible to hear or intercept conversations and communications without awareness of that interception... we have had an increase in the problem of protection of privacy and an increase of the problem of the security of the people in this country, as well as ***their ability to converse with the knowledge that it is a private matter and not one which is being overseen or overheard by other persons***."[18]

- Mr. Edward Broadbent (Oshawa-Whitby): "For the purpose of the debate, I define the right of privacy as the recognition of the legitimacy of man's ***right to think, to speak and to meet with people under circumstances from which all others but those whom he himself has selected are excluded***."[19]

- Mr. Terry O'Connor (Halton): "This bill should be looked upon, as it definitely is, as a codification of something which most people take for granted as a fundamental human right, that of protection of the personal privacy of the individual and ***his freedom from interference with his personal conversations***, his comings and goings, and his private affairs."[20]

---

[16] *TELUS*, *supra* at para. 31 per Abella J. (S.C.C.).

[17] *R. v. Jones*, 2016 ONCA 543 at para. 62.

[18] "Bill C-176, Protection of Privacy Bill: Creation of Offences Related to Interception of Private Communications by Certain Devices", 2nd reading, *House of Common Debates*, 29th Parl, 1st Sess, No 4 (May 7 1973) at 3471(Hon Otto E Lang) [emphasis added].

[19] Bill C-176, *supra* at 3481 [emphasis added].

[20] Bill C-176, *supra* at 3483 [emphasis added].

14. These statements support the proposition that Part VI of the *Criminal Code* was intended to provide enhanced protections for private communications as a class of information. It is consistent with this legislative objective to interpret "intercept" in Part VI precisely as it is drafted: "to listen to, record ***or acquire a communication or acquire the substance, meaning or purport thereof***".[21] This would include the act of acquiring the text messages that a telecommunications provider stores as part of the communications transmission process — even if the police do not seek the order to do so until a day, week or month after the communications come into existence. Regardless of when the police seek the order, they are ultimately acquiring the same thing: our private communications. The privacy interests at stake are the same. As Abella J. put it in *TELUS*, "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."[22]

15. Support for this approach can also be found in Moldaver J.'s concurring opinion in *TELUS*. As Moldaver J. noted, because the police requested that Telus produce text messages on a daily basis over a 13-day period, there was a 24-hour time delay between the communication of the text message and its retrieval by the police. (In fact, as Cromwell J. points out in dissent, some of the delays between the communications and their retrieval by the police lasted up to 72 hours.[23]) This delay, however, was insignificant to Moldaver J. In his view, "(t)o draw a line between what was authorized here and a Part VI intercept on the basis of such a theory is to draw 'an artificial and unrealistic distinction.'"[24] This supports the notion that "intercept" should not be temporally limited to acquisitions of text messages that are contemporaneous with the exchange of the message.

16. If the acquisition of a text message does not have to be contemporaneous with the making of the communication itself — and if a 24-hour (or 72-hour) delay between the making of the message and its retrieval by the police is immaterial — then it is difficult to see why Part VI would not apply to the police acquisition of text messages already in existence at the time they seek judicial authorization.

---

[21] *Criminal Code*, R.S.C., 1985, c. C-46, s. 183 [emphasis added].

[22] *TELUS*, *supra* at para. 36 per Abella J. (S.C.C.).

[23] *TELUS*, *supra* at paras. 183-184 per Cromwell J. (S.C.C.).

[24] *TELUS*, *supra* at para. 68 per Moldaver J. (S.C.C.).

17. The only difference between the acquisition of existing text messages and the acquisition of future text messages is the timing of when the police seek judicial authorizaiton. In the case of the former, the police apply for judicial authorization before — perhaps the day before — the targeted text messages come into existence. In the case of the latter, the police apply for judicial authorization after — perhaps the day after — the targeted text messages come into existence. In both cases, however, the police are asking the service provider to do the same thing: produce text messages that they have stored as part of their communications transmissions process. The investigative technique being authorized is the same. The only difference lies in when the police seek permission from the court. Cromwell J. made exactly this point in his dissenting opinion:

> Interception is a technique, a way of acquiring the substance of a private communication. I do not understand how it could be that exactly the same technique, which acquires information in exactly the same form, may be either a seizure of stored material or an interception, depending on the point in time at which the technique is authorized.[25]

18. The same point was made the post-*TELUS* case of *R. v. Croft*.[26] In *Croft*, the police relied on a production order to acquire the text messages stored in the servers of various service providers.[27] Burrows J. held that the police should have obtained a Part VI authorization instead.[28] Burrows J. reasoned that "if one accepts that to prospectively authorize the acquisition of text messages ***anticipated to be recorded*** is to authorize the interception of private communications", then one must also accept "that to authorize the acquisition of text messages ***previously recorded***…must also be to authorize the interception of private communications."[29]

19. The same conclusion was reached in the more recent case of *R. v. Hoelscher*.[30] In that case, Simpson J. considered this Court's opinions in *TELUS* and concluded that the police

---

[25] *TELUS*, *supra* at para. 158 per Cromwell J. (S.C.C.).

[26] *R. v. Croft*, [2013] A.J. No. 1231 (Q.B.).

[27] *R. v. Croft*, *supra* at paras. 6-7 (Alta. Q.B.).

[28] Burrows J. held that s. 487.012 was not intended to deal with private communications because it speaks *generally* to the production of "documents or data", whereas Part VI speaks *specifically* to the interception of "private communications": *R. v. Croft*, *supra* at paras. 60-61 (Alta. Q.B.). The same approach should be taken to s. 487(2.1), which speaks generally to the search of a computer system for "data". Parliament never intended for this provision to govern private communications. For recent authority for the principle of *generalia specialibus non derogant*, see *Great Lakes Power Ltd. v. Municipal Property Assessment Corp.*, [2012] O.J. No. 2870 at para. 153 (S.C.J.).

[29] *R. v. Croft*, *supra* at para. 47 (Alta. Q.B.) [emphasis added].

[30] *R. v. Hoelscher*, 2016 ABQB 44.

require a Part VI authorization to acquire text messages stored by a telecommunications provider regardless of when the police seek the authorization. He reasoned as follows:

> Notwithstanding the words "simultaneous" and "contemporaneous," 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.
>
> To give meaningful interpretation to the protections of Part VI, the Court must reject arbitrary temporal distinctions and concentrate on the privacy interest in the content of the communication.[31]

20. *Croft* and *Hoelscher* are admittedly in the minority when it comes to post-*TELUS* cases that have considered the question at issue in this appeal.[32] Their rationale, however, is persuasive. The applicability of Part VI should not turn on the timing of when the police seek judicial authorization to acquire text messages. Rather, the applicability of Part VI should turn on the substance of the investigative technique, which is the same regardless of whether the police seek the permission of the court before or after the text messages come into existence. Where the technique consists of the acquisition of text communications stored by a third party service provider, a Part VI authorization should be required.

---

[31] *R. v. Hoelscher*, *supra* at paras. 100, 103-104 (Alta. Q.B.).

[32] See *contra*, *R. v. Belcourt*, 2015 BCCA 126; *R. v. Webster*, 2015 BCCA 286; *R. v. Carty*, 2014 ONSC 212; *R. v. Pazder*, 2015 ABQB 493; *R. v. Vader*, 2016 ABQB 309.

II. THE SERVERS OF A THIRD PARTY SERVICE PROVIDER ARE DIFFERENT FROM THE DEVICE OF THE INTENDED RECIPIENT

21. The Crown respondents argue that if Part VI applies to the acquisition of text messages stored by a third party service provider, then Part VI must also apply to the acquisition of text messages from the personal devices of the parties to the communication.[33] The Crown's concern is misplaced. A distinction between the two investigative techniques is rooted in Abella J.'s opinion in *TELUS*:[34]

> 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***.[35]

22. Thus, while the plain language of Part VI suggests that it might apply to the acquisition of a text message from any computer (whether it belongs to the service provider or the end user), Abella J. interpreted "intercept" contextually to include a requirement that there be a connection between the acquisition of the text message and the communications process. This connection would only be made out when the police acquire the text messages from the third party service provider and not from the user's own device. In the case of the former, the text message is stored as part of the process of transmitting the communication to its intended recipient; in the case of the latter, the text message is only stored as a result of the successful completion of this process. Only the former is an "intercept".

23. The insistence on a connection between the text message and the communications process is a sensible limitation on the otherwise broad scope of the term "intercept". Once a text message is stored on the end user's device, they have some degree of control over it. The end

---

[33] Factum of the the Respondent, Her Majesty the Queen (in right of Ontario), paras. 89, 95; Factum of the Respondent, Her Majesty the Queen (in right of Canada), para. 109.

[34] Admittedly, the BCCLA took a different position when it intervened in *R. v. Fearon*, [2014] S.C.J. No. 77. However, that of course was before the Court issued its judgment in *Fearon*, which militates in favour of the narrower view of Part VI that the BCCLA advances in this factum.

[35] *TELUS*, *supra* at para. 37 (S.C.C.) [emphasis added].

user can retain the message on the device or delete it.[36] If the end user chooses to retain the message, then they have arguably made a decision that severs the connection between the message and the communications process that led to its storage on the user's device. In these circumstances, it makes sense that subsequent police acquisition of the message would not be considered an "intercept".

24. This approach also has the advantage of reconciling the broad language of Part VI with this Court's decision in *R. v. Fearon.* In *Fearon,* this Court held that the police can search a cell phone incident to arrest without a warrant in certain circumstances. In the course of doing so, the police may even review recently sent emails and text messages.[37] Thus, it cannot be that the mere acquisition of a private communication from a device attracts the protections of Part VI. At the same time, there is nothing in either the text or the purpose of Part VI that limits it to the acquisition of future text messages. The word "acquire" in the definition of "intercept" suggests the opposite. And so that cannot be the dividing line. The more sensible line is the one that Abella J. drew between the acquisition of text messages that have a sufficient connection to the communications process (*i.e.,* messages stored by the third party service provider) and the acquisition of text messages that do not (*i.e.,* message stored in the end user's device). Only the former attracts the application of Part VI.

25. Finally, this approach has the virtue of simplicity. The police need to know when they have to seek a Part VI authorization and when an ordinary search warrant will suffice. Under the approach that the BCCLA proposes, the police will be required to seek a Part VI authorization whenever they are acquiring text messages from a third party service provider. In contrast, other search powers (such as an ordinary search warrant) will suffice when the police are simply accessing the text messages on the user's personal device. This is a workable distinction that will be easy for the police to apply.

26. In summary, the BCCLA respectfully submits that the police should require a Part VI authorization whenever they acquire text messages from a third party service provider — even if

---

[36] While pressing the "delete" button does not immediately remove the text message from the device such that it cannot be retrieved by a forensic search, it does bring the deleted message one step closer to complete removal — eventually the device will need to overwrite data to clear up hard drive space, at which point the deleted message will truly be removed from the device: *R. v. Vu*, [2013] 3 S.C.R. 657 at para. 43.

[37] *R. v. Fearon*, *supra* at para. 76 (S.C.C.).

these messages have already been sent and received by the time the police seek judicial authorization. This approach strikes the optimal balance in all of the circumstances. It is sufficiently sensitive to law enforcement's need for clarity. It gives full effect to the broad language and purpose of Part VI to provide enhanced protections for our private communications. And it respects this Court's previous decisions in the area of digital privacy (*TELUS* and *Fearon*).

PART IV: SUBMISSIONS ON COSTS

27. The BCCLA does not seek costs and asks that none be awarded against it.

PART V: NATURE OF THE ORDER REQUESTED

28. The BCCLA does not request any orders.

All of which is respectfully submitted this 14th day of March, 2017.

GERALD CHAN
NADER R. HASAN
Stockwoods LLP
TD North Tower
77 King St. W., Suite 4130
Toronto, ON M5K 1H1

T: 416.593.1617
F: 416.593.9345
Email: GeraldC@stockwoods.ca
NaderH@stockwoods.ca

Counsel for the BCCLA

DAVID TAYLOR
Power Law LLP
130 Albert St., Suite 1103
Ottawa, ON
K1P 5G4

T: 613-702-5563
F: 1.888.404.2227
E: dtaylor@powerlaw.ca

Agent for the BCCLA

PART VI: TABLE OF AUTHORITIES

Authority Cited	Paragraph(s)
CASES	
R. v. Giles, [2007] B.C.J. No. 2918 (S.C.)	3
R. v. TELUS Communications Co., [2013] 2 S.C.R. 3	5, 7, 9, 11, 12, 14, 15, 17, 21
Re Rizzo & Rizzo Shoes Ltd., [1998] 1 S.C.R. 27	6
Lyons v. The Queen, [1984] 2 S.C.R. 633	7
R. v. Jones, 2016 ONCA 543	12
R. v. Croft, [2013] A.J. No. 1231 (Q.B.)	18
Great Lakes Power Ltd. v. Municipal Property Assessment Corp., [2012] O.J. No. 2870 (S.C.J.).	18
R. v. Hoelscher, 2016 ABQB 44	19
R. v. Belcourt, 2015 BCCA	20
R. v. Webster, 2015 BCCA 286	20
R. v. Carty, 2014 ONSC 212	20
R. v. Pazder, 2015 ABQB 493	20
R. v. Vader, 2016 ABQB 309	20
R. v. Fearon, [2014] S.C.J. No. 77	21, 24
R. v. Vu, [2013] 3 S.C.R. 657	23
SECONDARY SOURCES	
Matt Puzzo, "WhatsApp Encryption Said to Stymie Wiretap Order", *New York Times*, 12 March 2016	4
"Bill C-176, Protection of Privacy Bill: Creation of Offences Related to Interception of Private Communications by Certain Devices", 2nd reading, *House of Common Debates*, 29th Parl, 1st Sess, No 4 (May 7 1973) at 3471(Hon Otto E Lang)	13

PART VII: LEGISLATION CITED

A. Canadian Legislation

***Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c 11**

Fundamental freedoms 2. Everyone has the following fundamental freedoms: … (*b*) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; … Search or seizure 8. Everyone has the right to be secure against unreasonable search or seizure.	Libertés fondamentales 2. Chacun a les libertés fondamentales suivantes : … *b*) liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse et des autres moyens de communication; … Fouilles, perquisitions ou saisies 8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

***Criminal Code*, R.S.C. 1985, c. C-46**

PART VI Invasion of Privacy Definitions Definitions 183 In this Part, … *intercept* includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof; (*intercepter*) … *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; (*communication privée*)	PARTIE VI Atteintes à la vie privée Définitions Définitions … 183 Les définitions qui suivent s'appliquent à la présente partie. … *intercepter* S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet. (*intercept*) … *communication privée* Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine. (*private communication*)
Interception 184 (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. Saving provision (2) Subsection (1) does not apply to	Interception 184 (1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée. Réserve (2) Le paragraphe (1) ne s'applique pas aux personnes suivantes :

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;	a) une personne qui a obtenu, de l'auteur de la communication privée ou de la personne à laquelle son auteur la destine, son consentement exprès ou tacite à l'interception;
(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;	b) une personne qui intercepte une communication privée en conformité avec une autorisation ou en vertu de l'article 184.4, ou une personne qui, de bonne foi, aide de quelque façon une autre personne qu'elle croit, en se fondant sur des motifs raisonnables, agir en conformité avec une telle autorisation ou en vertu de cet article;
(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,	c) une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans l'un ou l'autre des cas suivants :
(i) if the interception is necessary for the purpose of providing the service,	(i) cette interception est nécessaire pour la fourniture de ce service,
(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or	(ii) à l'occasion de la surveillance du service ou d'un contrôle au hasard nécessaire pour les vérifications mécaniques ou la vérification de la qualité du service,
(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service;	(iii) cette interception est nécessaire pour protéger ses droits ou biens directement liés à la fourniture d'un service de communications téléphoniques, télégraphiques ou autres;
(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or	d) un fonctionnaire ou un préposé de Sa Majesté du chef du Canada chargé de la régulation du spectre des fréquences de radiocommunication, pour une communication privée qu'il a interceptée en vue d'identifier, d'isoler ou d'empêcher l'utilisation non autorisée ou importune d'une fréquence

(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for (i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or (ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).	ou d'une transmission; e) une personne - ou toute personne agissant pour son compte - qui, étant en possession ou responsable d'un ordinateur - au sens du paragraphe 342.1(2) -, intercepte des communications privées qui sont destinées à celui-ci, en proviennent ou passent par lui, si l'interception est raisonnablement nécessaire : (i) soit pour la gestion de la qualité du service de l'ordinateur en ce qui concerne les facteurs de qualité tels que la réactivité et la capacité de l'ordinateur ainsi que l'intégrité et la disponibilité de celui-ci et des données, (ii) soit pour la protection de l'ordinateur contre tout acte qui constituerait une infraction aux paragraphes 342.1(1) ou 430(1.1).
Application for authorization 185 (1) An application for an authorization to be given under section 186 shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 and shall be signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness or an agent specially designated in writing for the purposes of this section by (a) the Minister personally or the Deputy Minister of Public Safety and Emergency Preparedness personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or (b) the Attorney General of a province	Demande d'autorisation 185 (1) Pour l'obtention d'une autorisation visée à l'article 186, une demande est présentée *ex parte* et par écrit à un juge d'une cour supérieure de juridiction criminelle, ou à un juge au sens de l'article 552, et est signée par le procureur général de la province ou par le ministre de la Sécurité publique et de la Protection civile ou par un mandataire spécialement désigné par écrit pour l'application du présent article par : a) le ministre lui-même ou le sous-ministre de la Sécurité publique et de la Protection civile lui-même, si l'infraction faisant l'objet de l'enquête est une infraction pour laquelle des poursuites peuvent, le cas échéant, être engagées sur l'instance du gouvernement du Canada et conduites par le procureur général du Canada ou en son nom;

personally or the Deputy Attorney General of a province personally, in any other case,	b) le procureur général d'une province lui-même ou le sous-procureur général d'une province lui-même, dans les autres cas;
and shall be accompanied by an affidavit, which may be sworn on the information and belief of a peace officer or public officer deposing to the following matters:	il doit y être joint un affidavit d'un agent de la paix ou d'un fonctionnaire public pouvant être fait sur la foi de renseignements tenus pour véridiques et indiquant ce qui suit :
(c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence,	c) les faits sur lesquels le déclarant se fonde pour justifier qu'à son avis il y a lieu d'accorder une autorisation, ainsi que les détails relatifs à l'infraction;
(d) the type of private communication proposed to be intercepted,	d) le genre de communication privée que l'on se propose d'intercepter;
(e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,	e) les noms, adresses et professions, s'ils sont connus, de toutes les personnes dont les communications privées devraient être interceptées du fait qu'on a des motifs raisonnables de croire que cette interception pourra être utile à l'enquête relative à l'infraction et une description générale de la nature et de la situation du lieu, s'il est connu, où l'on se propose d'intercepter des communications privées et une description générale de la façon dont on se propose de procéder à cette interception;
(f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made,	f) le nombre de cas, s'il y a lieu, où une demande a été faite en vertu du présent article au sujet de l'infraction ou de la personne nommée dans l'affidavit conformément à l'alinéa e) et où la demande a été retirée ou aucune autorisation n'a été accordée, la date de chacune de ces demandes et le nom du juge auquel chacune a été présentée;
(g) the period for which the authorization is requested, and	g) la période pour laquelle l'autorisation est demandée;
(h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be	h) si d'autres méthodes d'enquête ont ou non été essayées, si elles ont ou non échoué, ou pourquoi elles paraissent avoir peu de chance de succès, ou si,

impractical to carry out the investigation of the offence using only other investigative procedures. Exception for criminal organizations and terrorist groups (1.1) Notwithstanding paragraph (1)(h), that paragraph does not apply where the application for an authorization is in relation to (a) an offence under section 467.11, 467.111, 467.12 or 467.13; (b) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or (c) a terrorism offence.	étant donné l'urgence de l'affaire, il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête. Exception dans le cas d'une organisation criminelle ou d'une infraction de terrorisme (1.1) L'alinéa (1)h) ne s'applique pas dans les cas où l'autorisation demandée vise : a) une infraction prévue aux articles 467.11, 467.111, 467.12 ou 467.13; b) une infraction commise au profit ou sous la direction d'une organisation criminelle, ou en association avec elle; c) une infraction de terrorisme.
Judge to be satisfied 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. Exception for criminal organizations and terrorism offences (1.1) Notwithstanding paragraph (1)(b), that paragraph does not apply where the judge is satisfied that the application for an authorization is in relation to (a) an offence under section 467.11, 467.111, 467.12 or 467.13;	Opinion du juge 186 (1) Une autorisation visée au présent article peut être donnée si le juge auquel la demande est présentée est convaincu que : a) d'une part, l'octroi de cette autorisation servirait au mieux l'administration de la justice; b) d'autre part, d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête. Exception dans le cas d'une organisation criminelle ou d'une infraction de terrorisme (1.1) L'alinéa (1)b) ne s'applique pas dans les cas où le juge est convaincu que l'autorisation demandée vise : a) une infraction prévue aux articles 467.11, 467.111, 467.12 ou 467.13; b) une infraction commise au profit ou

(b) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or (c) a terrorism offence.	sous la direction d'une organisation criminelle, ou en association avec elle; c) une infraction de terrorisme.