

SCC Court File No.: 37518

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR THE PROVINCE OF
NEWFOUNDLAND AND LABRADOR)

B E T W E E N:

SEAN PATRICK MILLS

APPELLANT

AND

HER MAJESTY THE QUEEN

RESPONDENT

AND

**DIRECTOR OF PUBLIC PROSECUTIONS, ATTORNEY GENERAL OF ONTARIO,
DIRECTOR OF CRIMINAL AND PENAL PROSECUTIONS OF QUÉBEC,
ATTORNEY GENERAL OF BRITISH COLUMBIA, ATTORNEY GENERAL OF
ALBERTA, SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC
INTEREST CLINIC, CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL
LAWYERS' ASSOCIATION, CANADIAN ASSOCIATION OF CHIEFS OF POLICE**

INTERVENERS

**FACTUM OF THE INTERVENER,
CANADIAN CIVIL LIBERTIES ASSOCIATION**
(Pursuant to Rule 42 of the Rules of the *Supreme Court of Canada*)

ADDARIO LAW GROUP LLP

171 John Street, Suite 101
Toronto, ON M5T 1X3

Frank Addario

Tel: (416) 649-5055
Fax: 1-866-714-1196
Email: faddario@addario.ca

James Foy

Tel: (416)646-1019
Fax: 1-866-714-1196
Email: jfoy@addario.ca

**Counsel for the Intervener,
Canadian Civil Liberties Association**

SUPREME ADVOCACY LLP

340 Gilmour St, Suite 100
Ottawa, Ontario
K2P 0R3

Eugene Meehan, Q.C.

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

**Ottawa Agent for the Intervener,
Canadian Civil Liberties Association**

SULLIVAN BREEN KING DEFENCE

Suite 300, Haymarket Square
223-233 Duckworth Street
St. John's, Newfoundland & Labrador
A1C 6N1

Rosellen Sullivan

Tel: (709) 739-4141
Fax: (709) 739-4145
E-mail: rsullivan@spdefence.ca

Counsel for the Appellant

**ATTORNEY GENERAL OF
NEWFOUNDLAND AND LABRADOR**

4th Floor, Atlantic Place
215 Water Street
St. John's, Newfoundland & Labrador
A1C 6C9

Lloyd M. Strickland

Tel: (709) 729-4299
Fax: (709) 729-1135
E-mail: lstrickland@gov.nl.ca

Counsel for the Respondent

**DIRECTEUR DES POURSUITES
CRIMINELLES ET PÉNALES DU QUÉBEC**

2828, boulevard Laurier, Tour 1
Bureau 500
Québec, Quebec G1V 0B9

Nicolas Abran

Ann Ellefsen-Tremblay
Tel: (418) 643-9059 Ext: 20934
Fax: (418) 644-3428
E-mail: nicolas.abran@dpcp.gouv.qc.ca

**Counsel for the Intervener, Director of
Criminal and Penal Prosecutions of Québec**

SPITERI & URSULAK LLP

1010 - 141 Laurier Avenue West
Ottawa, Ontario
K1P 5J3

Michael A. Crystal

Tel: (613) 563-1010
Fax: (613) 563-1011
E-mail: mac@sulaw.ca

Ottawa Agent for the Appellant

GOWLING WLG (CANADA) LLP

160 Elgin Street
Suite 2600
Ottawa, Ontario K1P 1C3

Robert E. Houston, Q.C.

Tel: (613) 783-8817
Fax: (613) 788-3500
E-mail: robert.houston@gowlingwlg.com

Ottawa Agent for the Respondent

**DIRECTEUR DES POURSUITES
CRIMINELLES ET PÉNALES DU
QUÉBEC**

17, rue Laurier
bureau 1.230
Gatineau, Quebec J8X 4C1

Sandra Bonanno

Tel: (819) 776-8111 Ext: 60446
Fax: (819) 772-3986
E-mail: sandra.bonanno@dpcp.gouv.qc.ca

**Ottawa Agent for Counsel for the
Intervener, Director of Criminal and
Penal Prosecutions of Québec**

ATTORNEY GENERAL OF ONTARIO

Crown Law Office - Criminal
720 Bay Street, 10th Floor
Toronto, Ontario
M7A 2S9

Katie Doherty

Susan Magotiaux

Tel: (416) 326-2302
Fax: (416) 326-4656
E-mail: katie.doherty@ontario.ca

Counsel for the Intervener, Attorney General of Ontario

PRESSER BARRISTERS

116 Simcoe Street, Suite100
Toronto, Ontario
M5H 4E2

Jill R. Presser

Tel: (416) 586-0330
Fax: (416) 596-2597
E-mail: presser@presserlaw.ca

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

STOCKWOODS LLP

TD North Tower, Toronto-Dominion Centre
77 King Street West, Suite 4130
Toronto, Ontario M5K 1H1

Gerald Chan

Tel: (416) 593-1617
Fax: (416) 593-9345
E-mail: geraldc@stockwoods.ca

Counsel for the Intervener, Criminal Lawyers Association

BORDEN LADNER GERVAIS LLP

World Exchange Plaza
100 Queen Street, suite 1300
Ottawa, Ontario
K1P 1J9

Nadia Effendi

Tel: (613) 237-5160
Fax: (613) 230-8842
E-mail: neffendi@blg.com

Ottawa Agent for Counsel for the Intervener, Attorney General of Ontario

SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC

University of Ottawa, Faculty of Law,
Common Law Section
57 Louis Pasteur Street
Ottawa, Ontario K1N 6N5

Tamir Israel

Tel: (613) 562-5800 Ext: 2914
Fax: (613) 562-5417
E-mail: tisrael@cippic.ca

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

POWER LAW

1103- 130 Albert Street
Ottawa, Ontario
K1P 5G4

Maxine Vincelette

Tel: (613) 702-5561
Fax: (613) 702-5561
E-mail: mvincelette@powerlaw.ca

Ottawa Agent for Counsel for the Intervener, Criminal Lawyers Association

**ROYAL NEWFOUNDLAND
CONSTABULARY**

Legal Services Unit
1 Fort Townshend
St. John's, Newfoundland & Labrador
A1C 2G2

Rachel Huntsman, Q.C.

Tel: (709) 729-8739
Fax: (709) 729-8214
E-mail: rachel.huntsman@rnc.gov.nl.ca

**Counsel for the Intervener , Canadian
Association of Chiefs of Police**

ATTORNEY GENERAL OF ALBERTA

3rd Floor, Centrium Place
300 - 332 6 Avenue, S.W.
Calgary, Alberta
T2P 0B2

Christine Rideout

Tel: (403) 297-6005
Fax: (403) 297-3453
E-mail: christine.rideout@gov.ab.ca

**Counsel for the Intervener, Attorney General
of Alberta**

**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:

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

**PERLEY-ROBERTSON, HILL &
MCDOUGALL**

1400 - 340 Albert Street
Ottawa, Ontario
K1R 0A5

Lynda A. Bordeleau

Tel: (613) 238-2022
Fax: (613) 238-8775
E-mail: lbordeleau@perlaw.ca

**Ottawa Agent for Counsel for the
Intervener, Canadian Association of
Chiefs of Police**

GOWLING WLG (CANADA) LLP

160 Elgin Street
Suite 2600
Ottawa, Ontario
K1P 1C3

D. Lynne Watt

Tel: (613) 786-8695
Fax: (613) 788-3509
E-mail: lynne.watt@gowlingwlg.com

**Ottawa Agent for Counsel for the
Intervener, Attorney General of Alberta**

GOWLING WLG (CANADA) LLP

160 Elgin Street
Suite 2600
Ottawa, Ontario
K1P 1C3

Robert E. Houston, Q.C.

Tel: (613) 783-8817
Fax: (613) 788-3500
E-mail: robert.houston@gowlingwlg.com

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

**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
E-mail: nick.devlin@ppsc-sppc.gc.ca

**Ottawa Agent for Counsel for the Intervener,
Director of Public Prosecutions**

**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
E-mail: francois.lacasse@ppsc-sppc.gc.ca

**Counsel for the Intervener, Director of
Public Prosecutions**

TABLE OF CONTENTS

<u>Tab</u>	<u>Page</u>
PART I – OVERVIEW	1
PART II – CCLA POSITION ON QUESTIONS ON APPEAL	1
PART III – STATEMENT OF ARGUMENT.....	2
A. Protecting a zone of privacy for electronic communications is essential	2
a) <i>The right to privacy includes the right to be left alone by the state.....</i>	<i>2</i>
b) <i>The normative approach to determining s. 8 claims.....</i>	<i>3</i>
B. <i>Marakah</i> provides a robust framework for deciding this case	3
a) <i>The normative approach to privacy requires a technologically-neutral</i> <i> approach.....</i>	<i>4</i>
b) <i>The reasonable expectation of privacy analysis is multi-factorial.....</i>	<i>5</i>
c) <i>A reasonable expectation of privacy is not dependent on confirming the</i> <i> identity of a co-conversationalist</i>	<i>7</i>
C. Practical law-enforcement concerns should not impact whether a reasonable	9
PART IV – SUBMISSIONS ON COSTS.....	10
PART V – NATURE OF THE ORDER REQUESTED.....	10
PART VI – TABLE OF AUTHORITIES.....	11

PART I – OVERVIEW

1. The question whether a claimant has a reasonable expectation of privacy in an electronic conversation impacts more than just standing before the Court; it is a much more fundamental question regarding whether Canadians can expect a zone of privacy for one-to-one digitally-mediated conversations. As Doherty J.A. recently put it: “A finding that a claimant has a reasonable expectation of privacy is not only a description of a specific constellation of factual considerations, but is also a declaration of societal aspirations and values.”¹

2. A zone of privacy for electronic conversations, whether conducted via text message or other means, is essential to the functioning of a free and democratic society. The state should not be permitted to take advantage of the anonymity offered by electronic communications and the digital world in order to surreptitiously record conversations with people at its sole discretion.

3. The Canadian Civil Liberties Association urges the Court to re-affirm the normative and technologically-neutral approach it took to privacy in *R. v. Marakah*.² Requiring a person to definitively identify their interlocutor before they are entitled to privacy in an electronic conversation effectively re-introduces a risk analysis approach to s. 8 of the *Charter*. Such an approach has been consistently rejected by this Court and should again be rejected in this case. Relationships formed online are no less worthy of privacy protection than those formed in physical space, and in both cases, even individuals who choose not to self-identify still deserve to hold conversations free of intrusion by the state.

4. The Court should also clarify that law-enforcement aspirations are not relevant to the reasonable expectation of privacy analysis. These interests should only be taken into account when determining if the search was authorized by law or whether evidence should be excluded as the result of a breach of *Charter* rights.

5. The CCLA takes no position on the facts.

PART II – CCLA POSITION ON QUESTIONS ON APPEAL

6. The CCLA submits:

(1) People have a reasonable expectation of privacy in one-to-one electronic communications, regardless of the technological medium used to facilitate the

¹ *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, at para. 41.

² *R. v. Marakah*, 2017 SCC 59, [2017] 2 SCR 608.

conversation. The reasonable expectation of privacy analysis under s. 8 must be technologically-neutral. The focus is on the nature of the communications, not on the medium in which it takes place;

- (2) A person does not have to confirm the identity of their interlocutor in order to have a reasonable expectation of privacy in their conversation. Such a requirement would be inconsistent with Canadian values of privacy in the digital age because it would undermine a person's ability to choose what information they share, and with whom they share that information. It would also re-introduce the risk analysis rejected by this Court in *Duarte*;
- (3) Law-enforcement goals are not relevant at the standing stage of the s. 8 analysis.

PART III – STATEMENT OF ARGUMENT

A. Protecting a zone of privacy for electronic communications is essential

a. The right to privacy includes the right to be left alone by the state

7. Privacy encompasses both the “right to be left alone by other people” and the “right to be left alone by the state.”³ People should be free to express themselves and form relationships without the prying eye of the public or the fear of state intrusion. As argued by Professor Austin, the protection of a private space in which to be “distinct individuals” and to have an “authentic inner life and intimate relationships” is essential to the conception of privacy.⁴ Professor Stewart also emphasizes the need to protect private spaces:

To be free to think and to form beliefs and opinions requires not just public spaces for expression and debate but also private spaces for thought and contemplation, for reading controversial and uncontroversial material alike, for exploring with friends and colleagues ideas that may later be qualified or rejected.⁵

8. The reasons for protecting private spaces apply equally to Canadians’ physical and digital lives. Digital devices and electronic communications provide a myriad of ways for self-fulfillment and expression. They allow people to reach beyond their immediate surroundings and form relationships and communities with others around the world. They enable self-expression and debate. Protecting a zone of privacy for people to communicate through electronic means enables individuals to make meaningful choices about their

³ *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696 at para. 39; *Orlandis-Habsburgo*, at para. 42.

⁴ L. Austin, “Privacy and the Question of Technology” (2003), 22 *Law & Phil.* 119, at pp. 146-47 [“Privacy and the Question of Technology”].

⁵ H. Stewart, “Normative Foundations for Reasonable Expectations of Privacy” (2001) 54 *S.C.L.R.* 335, at p. 345 [“Normative Foundations”].

participation in society: “A private inner life is essential to the autonomous individual that forms the basis of a free and democratic society as envisioned by the *Charter*.”⁶

b. The normative approach to determining s. 8 claims

9. The Supreme Court has consistently affirmed that the reasonable expectation of privacy standard is normative, rather than descriptive.⁷ A normative approach to privacy ensures that the focus of the court’s inquiry is on values as opposed to technical mechanisms.

10. The normative approach to privacy is focussed on whether Canadian values permit an intrusion on privacy without complying with the reasonableness standard in s. 8 of the *Charter*.⁸ If the state conduct in question undermines Canadian privacy values, the state must meet a burden of constitutionally justifying its conduct.⁹ Professor Stewart describes the inquiry this way:

[T]he ultimate normative question is whether, in light of the impact of an investigative technique on privacy interests, it is right that the state should be able to use that technique without any legal authorization or judicial supervision. Does our conception of the proper relationship between the investigative branches of the state and the individual permit this technique without specific legal authorization?¹⁰

11. The normative question at issue in this case and others like it is: Can an agent of the state surreptitiously engage in and record conversations with people online without legal authorization or judicial supervision?

12. The CCLA submits that the answer to that question is no. The privacy interest that people have in their electronic communications is too high to allow agents of the state unfettered discretion to engage in and record such conversations with any member of the public.

B. *Marakah* provides a robust framework for deciding this case

13. The normative question at issue in this case should be answered by applying the framework articulated in *Marakah*: (1) What was the subject matter of the alleged search? (2)

⁶ *R. v. Fearon*, 2014 SCC 77, [2014] S.C.R. 621, *per* Karakatsanis J. (in dissent but not on this point) at para. 115.

⁷ *R. v. Tessling*, [2004] 3 S.C.R. 432, 2004 SCC 67, at para. 42; *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 18; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 14; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34.

⁸ *R. v. Orlandis-Habsburgo*, at para. 42.

⁹ *R. v. Ward*, 2012 ONCA 660, at para. 82.

¹⁰“Normative Foundations”, at p. 342.

Did the claimant have a direct interest in the subject matter? (3) Did the claimant have a subjective expectation of privacy in the subject matter? (4) If so, was the claimant's subjective expectation of privacy objectively reasonable?¹¹ The *Marakah* framework is technologically-neutral and applies broadly to all claims in which a person is claiming a reasonable expectation of privacy in communications that have been seized by the state.¹²

a. *The normative approach to privacy requires a technologically-neutral approach*

14. Person-to-person communication tools all use different ways of transmitting, storing, and displaying electronic messages. New mediums for electronic conversation are continuously being developed. A normative approach to privacy is resistant to these technical differences and must focus on the real question: does the claimant have a reasonable expectation of privacy in the electronic conversation at issue? As stated by Abella J. in *TELUS*, “[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications.”¹³

15. Applying a technologically-neutral approach in *Marakah* led the Court to conclude that the subject matter of the search was the electronic conversation itself and that the claimant had a reasonable expectation of privacy in the subject matter of the search.¹⁴ Framing the subject matter of the search to identify what the police are really after – the electronic conversation – is an essential first step in the s. 8 analysis.

16. The same approach also impacts the question of whether a claimant has an objectively reasonable expectation of privacy. The key holding in *Marakah* that the claimant's text message conversations attracted an *objectively* reasonable expectation of privacy applies equally to cases in which the claimant uses a different medium for person-to-person electronic conversation. The specific technical means by which a conversation is carried out is not relevant to determining whether a person's expectation of privacy in that conversation is an objectively reasonable one. While Chief Justice McLachlin stated that whether a text message conversation will attract a reasonable expectation of privacy is fact-specific and determined on a case-by-case basis, this comment must be understood in context.¹⁵

¹¹ *Marakah*, at para. 11.

¹² *Marakah*, at para. 19.

¹³ *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3, at para. 5. See also *R. v. Wong*, [1990] 3 S.C.R. 36, at p. 44.

¹⁴ *Marakah*, at para. 20.

¹⁵ *Marakah*, at para. 5.

17. First, whether a claimant has a reasonable expectation of privacy is assessed in the totality of the circumstances.¹⁶ Second, this totality of the circumstances must include Chief Justice McLachlin's distinction in *Marakah* between private person-to-person electronic communication and participating in more public forums using electronic means. The Chief Justice gave examples of electronic messages that might not attract a reasonable expectation of privacy: "for example, messages posted on social media, conversations occurring in crowded internet chat rooms, or comments posted on online messages boards."¹⁷ In other words, participating in a public forum online may not attract an objectively reasonable expectation of privacy.

18. However, engaging in an electronic conversation with another person *does* attract an objectively reasonable expectation of privacy. There is no principled reason to distinguish the holding in *Marakah* that text message conversations attract a reasonable expectation of privacy on the basis that an electronic conversation took place over a different medium. Accordingly, *Marakah* provides a framework for assessing s. 8 standing claims in all cases involving electronic conversations or communications, not just text messages. The focus of the inquiry is on the private nature of the communication, not on the particular medium used to facilitate that communication.

19. As has been repeatedly recognized by this court, the focus of the s. 8 inquiry is not on the actual contents of the electronic messages seized by the police but on the *potential* for an electronic conversation to reveal personal or biographical information.¹⁸ As held by Chief Justice McLachlin, "it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging."¹⁹ The same is true of other mediums for person-to-person electronic conversations.

b. The reasonable expectation of privacy analysis is multi-factorial

20. Courts have identified numerous factors for determining whether an objectively reasonable expectation of privacy exists in different circumstances.²⁰ In *Marakah*, this Court

¹⁶ *Marakah*, at paras. 10-11; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 39, *Spencer*, at paras. 16-18; *Patrick*, at para. 26; *Tessling*, at para. 19.

¹⁷ *Marakah*, at para. 55.

¹⁸ *Marakah*, at para. 32; *Patrick*, at para. 32; *Wong*, at p. 50; *Cole*, at para. 47; *Tessling*, at para. 25.

¹⁹ *Marakah*, at para. 34.

²⁰ *Cole*, at para. 45; *Tessling*, at para. 32; *R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 45; *Marakah*, at para. 24.

focussed on three: the place where the search occurred; the private nature of the information; and control over the subject matter.²¹

21. The private nature of the information is particularly important in cases in which the subject matter of the search concerns informational privacy. As stated by Sopinka J., s. 8 of the *Charter* protects a “biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state.”²² The degree to which the information sought by the state tends to reveal personal information guides the normative analysis: “the more personal and confidential the information, the more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.”²³

22. The holdings in *Marakah* about the personal nature of text messaging should apply equally to all mediums of one-to-one electronic conversation. Just like text messages, many other electronic communication tools such as e-mail, Google Hangouts, Facebook Messenger, or WhatsApp are designed to facilitate one-on-one private conversations. The information sent over these platforms is intended to be received only by the people to whom the messages are sent. People may be inclined to discuss highly private matters using these platforms *because* the platforms are understood to be private.²⁴ Indeed, just like text messages, “[t]here is no more discreet form of correspondence” than electronic messaging platforms.²⁵ As in *Marakah*, it is reasonable for people to expect that such interactions, regardless of the electronic medium used to send those interactions, will remain private.

23. Control “is not dispositive, but only one factor to be considered in the totality of the circumstances” when assessing reasonable expectations of privacy in an electronic conversation.²⁶ As per *Marakah*, “[a]n individual does not lose control over information for the purposes of s. 8 of the *Charter* simply because another individual possesses it or can access it.”

²¹ *Marakah*, at para. 24.

²² *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293.

²³ *Cole*, at para. 45.

²⁴ *Marakah*, at para. 34.

²⁵ *Marakah* at para. 35.

²⁶ *Marakah*, at para. 44.

c. *A reasonable expectation of privacy is not dependent on confirming the identity of co-conversationalists*

24. The focus of the reasonable expectation of privacy analysis must remain on the subject matter: the electronic conversation itself. The risk that a party to that conversation will share that conversation with the state, or is in fact an agent of the state, changes nothing about the private nature of the conversation itself and the reasonable expectation that it will remain private. This holds true whether or not such an individual knows with complete certainty the identity of a communicant on the other end of a digital communication.

25. A focus on whether there is a risk that the information could be shared with the state ignores the normative focus of the s. 8 inquiry: whether the state should be allowed to seize information without constitutional scrutiny. As stated by La Forest J. in *Duarte*:

[T]he question whether to regulate participant surveillance cannot logically be made to turn on the expectations of individuals as to whether their interlocutor will betray their confidence. No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being.²⁷

26. Despite this Court's admonitions, the Newfoundland and Labrador Court of Appeal adopted the risk analysis in this case: the court held that a person does not have a reasonable expectation of privacy because it was risky to communicate with a person whose identity he or she cannot confirm over electronic social media.²⁸

27. As held in *Marakah*, the arbitrary exercise of state power cannot rest on the risk that a participant will share that information with the state: "the risk that a recipient could disclose an electronic conversation does not negate a reasonable expectation of privacy in an electronic conversation."²⁹ Similarly, the risk that a recipient is not who they say they are also does not negate a reasonable expectation of privacy. A person is not required to confirm or attempt to confirm the identity of a communicant in order to have a private conversation with them. To hold otherwise ignores the realities of our digital world.

28. Relationships online are no less worthy of privacy protection than relationships formed at the grocery store or the local pub, regardless of whether the parties to the communication choose to share their real identities. Electronic communication tools are used

²⁷ *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 49.

²⁸ *R. v. Mills*, 2017 NLCA 12, at para. 23.

²⁹ *Marakah*, at para. 40.

to communicate beyond a person's immediate surroundings with people from around the world. Requiring a person to confirm a co-conversationalist's identity in the "real world" – and, by logical extension, to disclose their own identity – in order to expect privacy in a conversation would ignore the rapid technological change taking place in society and would introduce new and troubling identity-verification requirements for electronic conversations that exceed those in the pre-digital age. Such an approach to privacy would ignore the reality of how Canadians use the Internet and electronic communications. A zone of privacy to engage in social activities through electronic means is essential to the fulfillment of a private inner life, and engaged social participation.

29. The reasonable expectation of privacy analysis does not change because one of the participants to the conversation is an agent of the state. The risk that a communicant will share a person's confidences *with the state* does not justify unregulated state access to our conversations; the risk that a communicant *is an agent of the state* cannot justify the same. Adopting such an approach would be directly contrary to this Court's conclusion in *Duarte*:

Our perception that we are protected against arbitrary interceptions of private communications ceases to have any real basis once it is accepted that the state is free to record private communications, without constraint, provided only that it has secured the agreement of one of the parties to the communication. Since we can never know if our listener is an informer, and since, if he proves to be one, we are to be taken to be tacitly consenting to the risk that the state may be listening to and recording our conversations, we should be prepared to run this risk every time we speak.³⁰ [Emphasis added.]

30. The ability to maintain some degree of anonymity is integral to ensuring privacy.³¹ The value of anonymity extends beyond anonymous browsing and includes the ability to converse, debate, and explore ideas with others. The possibility of unknowingly communicating with an agent of the state, absent judicial authorization, seriously erodes a person's ability to live an authentic, private life. As articulated by Professor Austin, this "loss of privacy occurs because we feel the pressure to conform to public norms."³² The wrong is not "had we known we would have acted differently. For acting differently in such a case would mean acting publicly, which itself involves a loss of privacy."³³ As La Forest J. states:

³⁰ *Duarte*, at p. 47.

³¹ *R. v. Spencer*, at para. 42; *Ward*, at para. 71.

³² "Privacy and the Question of Technology", at pp. 146-47.

³³ "Privacy and the Question of Technology", at pp. 146-47.

“we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.”³⁴

31. Such a loss of privacy is antithetical to Canadian values. Individuals must be free to choose what information they share, and with whom they share that information.³⁵ Requiring an individual to share their identity, and confirm the identity of their communicant, would place them in a Catch-22 situation. In order to maintain a reasonable expectation of privacy, they would need to share and demand information that they may want to remain private. Such a situation would require Canadians to become “digital recluses in order to maintain some semblance of privacy in their lives.”³⁶ That approach is unjustifiable given this Court’s conclusions in *Duarte*, *Marakah* and *Jones*.

32. Holding that there is a reasonable expectation of privacy in an electronic conversation in any given case is not the end of the inquiry. The normative question underlying the reasonable expectation of privacy is whether “the personal privacy claim advanced ... must ... be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society.”³⁷

33. It is always open for the state to justify its conduct by demonstrating that a search and seizure was not unreasonable, or by arguing that evidence obtained should be admitted under s. 24(2) of the *Charter*. As held in *Marakah*, “[s]tanding is merely the opportunity to argue one’s case.”³⁸ While concluding that standing exists in any particular case does not decide that case, it also serves as “a declaration of societal aspirations and values” more broadly.³⁹ It sends a crucial message to Canadians that they can expect a zone of privacy over their electronic conversations.

C. Practical law-enforcement concerns should not impact whether a reasonable expectation of privacy exists

34. Law enforcement uses many techniques to combat crime in the digital world. Concluding that an individual can have a reasonable expectation of privacy in electronic conversations with undercover police officers will undoubtedly impact the use of some of

³⁴ *R. v. Wong*, at p. 47.

³⁵ *Fearon*, at para. 114.

³⁶ *Jones*, at para. 45.

³⁷ *Ward*, at para. 87.

³⁸ *Marakah*, at para. 51.

³⁹ *Orlandis-Habsburgo*, at para. 41.

these law-enforcement techniques. Lawful authority for searching and seizing such communications would need to be obtained.

35. But these practical concerns do not impact the reasonable expectation of privacy stage of the analysis. The focus of the expectation of privacy stage of the analysis is on the societal values that are furthered by the protection of privacy. While this Court has referred to the s. 8 analysis as “striking the balance” between the public’s interest in being left alone and the government’s interest in law enforcement, this balance is not struck within the analysis of whether a person has standing to bring a s. 8 claim.⁴⁰ As held by Doherty J.A. in *R. v. Orlandis-Habsburgo*:

I make one last point about the normative nature of the reasonable expectation of privacy inquiry. The societal values furthered by personal privacy are central to the inquiry. However, other values may also have an impact on that inquiry. I am not referring here to state interests such as law enforcement. Those interests are taken into account in the reasonableness assessment which follows a determination that a reasonable expectation of privacy exists.⁴¹

36. The law enforcement interests in police investigations using the Internet and electronic communications thus belong in latter stages of the s. 8 analytical framework. These investigative techniques may be reasonable if they have prior judicial authorization or if Parliament creates police powers specifically enabling them. But the fact that the police seek to use these investigative techniques cannot overwhelm the analysis of whether there is a reasonable expectation of privacy in electronic conversations.

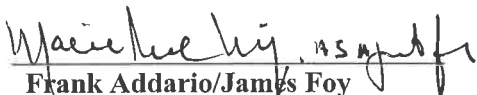
PART IV – SUBMISSIONS ON COSTS

37. The CCLA does not seek costs and asks that none be awarded against it.

PART V – NATURE OF THE ORDER REQUESTED

38. The CCLA makes no submissions on the ultimate order to be made.

ALL OF WHICH IS RESPECTFULLY SUBMITTED, this 10th day of May, 2018.


Frank Addario/James Foy

⁴⁰ *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 159-60; *Tessling*, at paras. 17-18.

⁴¹ *Orlandis-Habsburgo*, at para. 47.

PART VI – TABLE OF AUTHORITIES

CASES	PARAGRAPH(S)
<i>Hunter v. Southam Inc.</i> , [1984] 2 S.C.R. 145	35
<i>R. v. Cole</i> , 2012 SCC 53, [2012] 3 S.C.R. 34	17, 20, 21
<i>R. v. Duarte</i> , [1990] 1 S.C.R. 30	25, 29
<i>R. v. Edwards</i> , [1996] 1 S.C.R. 128	20
<i>R. v. Fearon</i> , 2014 SCC 77, [2014] S.C.R. 621	8, 31
<i>R. v. Gomboc</i> , 2010 SCC 55, [2010] 3 S.C.R. 211	9
<i>R. v. Jones</i> , 2017 SCC 60, [2017] 2 S.C.R. 696	7, 31
<i>R. v. Marakah</i> , 2017 SCC 59, [2017] 2 SCR 608	3, 13, 15, 16, 17, 19, 20, 23, 27, 33
<i>R. v Mills</i> , 2017 NLCA 12	26
<i>R. v. Plant</i> , [1993] 3 S.C.R. 281	21
<i>R. v. Orlandis-Habsburgo</i> , 2017 ONCA 649	1, 7, 33, 35
<i>R. v. Patrick</i> , 2009 SCC 17, [2009] 1 S.C.R. 579	9, 17
<i>R. v. Spencer</i> , 2014 SCC 43, [2014] 2 S.C.R. 212	9, 17, 30
<i>R. v. TELUS Communications Co.</i> , 2013 SCC 16, [2013] 2 S.C.R. 3	14
<i>R. v. Tessling</i> , [2004] 3 S.C.R. 432, 2004 SCC 67	9, 17, 19, 20, 35
<i>R. v. Ward</i> , 2012 ONCA 660	10, 32
<i>R. v. Wong</i> , [1990] 3 S.C.R. 36	14, 19, 30

SECONDARY SOURCES	PARAGRAPH(S)
L. Austin, “Privacy and the Question of Technology” (2003), 22 <i>Law & Phil.</i> 119	7, 30
H. Stewart, “Normative Foundations for Reasonable Expectations of Privacy” (2001) 54 <i>S.C.L.R.</i> 335	7, 9