SCC Court File No: 37518

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

B E T W E E N:

SEAN PATRICK MILLS

APPELLANT
(Respondent)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(Appellant)

- and -

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

INTERVENERS

FACTUM OF THE INTERVENER, SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Presser Barristers
116 Simcoe Street, Suite 116
Toronto, Ontario, M5H 4E2

Jill R Presser

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

Markson Law Professional Corporation
390 Bay Street, Suite 1000
Toronto, Ontario, M5H 2Y2

Kate Robertson

Tel: (416) 800-0502
Fax: (416) 601-2514
Email: krobertson@marksonlaw.com

Counsel for the Intervener

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML Section
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tamir Israel

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

Agent for the Intervener

TO: **THE REGISTRAR**

COPY TO:

SULLIVAN BREEN KING DEFENCE
Suite 300, Haymarket Square
223-233 Duckworth Street
St. John's, NL, A1C 1G8

Rosellen Sullivan

Tel: (709) 700-1801
Fax: (709) 739-4145
Email: rsullivan@spdefence.ca

Counsel for the Appellant, Sean Patrick Mills

SPITERI & URSULAK LLP
1010-141 Laurier Ave. W.
Ottawa, ON K1P 5J3

Michael A. Crystal

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

Agent for the Appellant, Sean Patrick Mills

AND TO:

ATTORNEY GENERAL OF NEWFOUNDLAND AND LABRADOR
4th Floor, Atlantic Place
251 Water Street
St. John's, NL, A1C 6C9

Lloyd Strickland
Sheldon B. Steeves

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

Counsel for the Respondent, Her Majesty the Queen

GOWLING WLG (CANADA) LLP
160 Elgin Street, Suite 2600
Ottawa, ON K1P 1C3

Robert E. Houston, Q.C.

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

Agent for the Respondent, Her Majesty the Queen

AND TO:

DIRECTEUR DES POURSUITES CRIMINELLES ET PÉNALES DU QUÉBEC
2828, boulevard Laurier, Tour 1
Bureau 500
Québec, QC 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

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

Sandra Bonanno

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

	Counsel for the Intervener, Director of criminal and penal prosecutions of Québec	**Agent for the Intervener, Director of criminal and penal prosecutions of Québec**
AND TO:	**ATTORNEY GENERAL OF ONTARIO** Crown Law Office - Criminal 720 Bay Street, 10th Floor Toronto, ON M7A 2S9 Katie Doherty Susan Magotiaux Tel: (416) 326-2302 FAX: (416) 326-4656 E-mail: katie.doherty@ontario.ca	**BORDEN LADNER GERVAIS LLP** World Exchange Plaza 100 Queen Street, suite 1300 Ottawa, ON K1P 1J9 Nadian Effendi Tel: (613) 237-5160 FAX: (613) 230-8842 E-mail: neffendi@blg.com
	Counsel for the Intervener, Attorney General of Ontario	**Agent for the Intervener, Attorney General of Ontario**
AND TO:	**ADDARIO LAW GROUP** 171 John Street, Suite 101 Toronto, ON M5T 1X3 Frank Addario James Foy Tel: (416) 649-5055 FAX: (866) 714-1196 E-mail: faddario@addario.ca	**SUPREME ADVOCACY LLP** 100 - 340 Gilmour Street Ottawa, ON K2P 0R3 Eugene Meehan, Q.C. Tel: (613) 695-8855 Ext: 101 FAX: (613) 695-8580 E-mail: emeehan@supremeadvocacy.ca
	Counsel for the Intervener, Canadian Civil Liberties Association	**Agent for the Intervener, Canadian Civil Liberties Association**
AND TO:	**STOCKWOODS LLP** TD North Tower, Toronto-Dominion Centre 77 King Street West, Suite 4130 Toronto, ON M5K 1H1 Gerald Chan Tel: (416) 593-1617 FAX: (416) 593-9345 E-mail: geraldc@stockwoods.ca	**POWER LAW** 130 Albert Street Suite 1103 Ottawa, ON K1P 5G4 Maxine Vincelette Tel: (613) 702-5561 FAX: (613) 702-5561 E-mail: mvincelette@powerlaw.ca
	Counsel for the Intervener, Criminal Lawyers' Association	**Agent for the Intervener, Criminal Lawyers' Association**
AND TO:	**ROYAL NEWFOUNDLAND CONSTABULARY**	**PERLEY-ROBERTSON, HILL & MCDOUGALL**

	Legal Services Unit, 1 Fort Townshend St. John's, NFLD A1C 2G2	1400 - 340 Albert Street Ottawa, ON K1R 0A5
	Rachel Huntsman, Q.C.	Lynda A. Bordeleau
	Tel: (709) 729-8739 FAX: (709) 729-8214 E-mail: rachel.huntsman@rnc.gov.nl.ca	Tel: (613) 238-2022 FAX: (613) 238-8775 E-mail: lbordeleau@perlaw.ca
	Counsel for the Intervener, Canadian Association of Chiefs of Police	**Agent for the Intervener, Canadian Association of Chiefs of Police**
AND TO:	**ATTORNEY GENERAL OF ALBERTA** 3rd Floor, Centrium Place 300 - 332 6 Avenue, S.W. Calgary, AB T2P 0B2	**GOWLING WLG (CANADA) LLP** 160 Elgin Street, Suite 2600 Ottawa, ON K1P 1C3
	Christine Rideout	D. Lynne Watt
	Tel: (403) 297-6005 FAX: (403) 297-3453 E-mail: christine.rideout@gov.ab.ca	Tel: (613) 786-8695 FAX: (613) 788-3509 E-mail: lynne.watt@gowlingwlg.com
	Counsel for the Intervener, Attorney General of Alberta	**Agent for the Intervener, Attorney General of Alberta**
AND TO:	**ATTORNEY GENERAL OF BRITISH COLUMBIA** 3rd Floor - 940 Blanshard Street Victoria, BC V8W 3E6	**GOWLING WLG (CANADA) LLP** 160 Elgin Street Suite 2600 Ottawa, ON K1P 1C3
	Daniel M. Scanlan	Robert E. Houston, Q.C.
	Telephone: (250) 387-0284 FAX: (250) 387-4262	Telephone: (613) 783-8817 FAX: (613) 788-3500 E-mail: robert.houston@gowlingwlg.com
	Counsel for the Intervener, Attorney General of British Columbia	**Agent for the Intervener, Attorney General of British Columbia**
AND TO:	**PUBLIC PROSECUTION SERVICE OF CANADA** 130 King Street West Suite 3400, Box 36 Toronto, ON M5X 1K6	**DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA** 160 Elgin Street 12th Floor Ottawa, ON K1A 0H8
	Nicholas E. Devlin	François Lacasse

Tel: (416) 952-6213
FAX: (416) 952-2116
E-mail: nick.devlin@ppsc-sppc.gc.ca

Counsel for the Intervener, Director of Public Prosecutions

Tel: (613) 957-4770
FAX: (613) 941-7865
E-mail: francois.lacasse@ppsc-sppc.gc.ca

Agent for the Intervener, Director of Public Prosecutions

TABLE OF CONTENTS

PART I. OVERVIEW AND STATEMENT OF FACTS

1. This appeal raises the issue of whether constitutional safeguards are required where the police falsify an online identity and surreptitiously interpose themselves into, and make recordings of, electronic conversations. The state asserts an unregulated discretion to use online undercover techniques without judicial oversight or relying on any express authorization under the *Criminal Code*. This is notable because where the use of the technique has surfaced to the attention of the criminal courts, it is being used to engage in online fishing expeditions in the hope of uncovering crime—a prospect that is normally looked upon with disapprobation when it comes to the use of surveillance in a free society.[1] Despite the utility of good old-fashioned undercover police work, the validity of law enforcement goals has not before permitted an intrusive electronic surveillance technique to be immune from judicial oversight.

2. The failure of the state to seek judicial oversight for this police technique is significant in light of the potential reach of the surveillance. Online undercover investigations can be breathtakingly invasive in scope. Electronic communications are ubiquitous in our society. They create a host of technological opportunities that the police may attempt to exploit undetected. A police officer can falsify identity or even impersonate a real identity known to a target. No consent is required from the civilian "informant" whose identity is employed. Without judicial oversight, no temporal limits are placed on the surveillance, nor are there limits on the use or retention of the private information obtained. Using the false profile, the police can then originate communications, or interject themselves into the middle of the electronic conversations that all judges in *R. v. Marakah* recognized may engage a reasonable expectation of privacy.[2]

3. The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC") submits that the Court of Appeal for Newfoundland erred in deciding that there was no reasonable expectation of privacy in one-on-one digital text-based communications, because the Appellant took

---

[1] *R. v. Jones*, [2017] 2 S.C.R. 696, at para. 74, citing *R. v. Finlay* (1985), 23 C.C.C. (3d) 48 (Ont. C.A.), at p. 70

[2] *R. v. Marakah*, [2017] 2 S.C.R. 608, per McLachlin C.J., at paras 31-37; per Rowe J. concurring with the majority, at para. 88; per Moldaver J. for the dissent, at paras. 92-93

"a risk"[3] in communicating online with an individual that he did not know. The reasonableness of an expectation of privacy in an electronic, one-on-one conversation does not depend on whether the two individuals have met face-to-face. Nor does the fact that an electronic conversation is typed (rather than spoken) negate a reasonable expectation of privacy. In a free society, the right to be secure against unreasonable search and seizure means that the police must not be left with an unlimited discretion to falsify online identities, inject themselves into one-on-one conversations, and determine the scope and duration of such intrusive activities.

4. CIPPIC makes no submissions on the facts of this appeal.

PART II. POSITION ON QUESTIONS IN ISSUE

5. CIPPIC submits the following:

i. The content of electronic, one-on-one conversations has the potential to reveal core biographical information about an individual. This is so even and especially amongst two individuals who have never met in person. As such, electronic conversations between "strangers" may still be private communications protected under Part VI of the *Criminal Code* and s. 8 of the *Charter*.

ii. It is the content of the communication and not the vagaries of the particular communications medium that should determine whether communications are private. Individuals may exercise a range of remote controls over spoken and text-based messages sent to another device. Some text-based communications are as technologically fleeting as spoken communications, while some spoken communications create "records" that are wholly analogous to text-based communications. The loss of absolute control over spoken and written communications should not deprive the interlocutor of a reasonable expectation of privacy from state intrusion in *either* form of communication.

iii. The normative approach required of section 8 must guard against an imputed assumption to all individuals in society that a state agent is interjecting in our private, electronic conversations and making a permanent record of those conversations.

PART III. STATEMENT OF ARGUMENT

A. The normative question of whether there is a reasonable expectation of privacy in an electronic conversation does not depend on whether individuals have met in person

6. In *R. v. Marakah*, this Court set out a framework for analyzing the objective reasonableness of an expectation of privacy in a one-on-one electronic conversation. CIPPIC submits that in assessing

[3] *R. v. Mills*, 2017 NLCA 12, at para. 23 ("*Mills*, CA Decision")

the totality of the circumstances, including the private nature of the information, the fact that electronic communications take place between two individuals who have not met does not displace a reasonable expectation of privacy in the conversation.

7. This Court has long held that the reasonable expectation of privacy standard is normative, not descriptive.[4] As recognized in *R v. M (A):*

> Section 8, like the rest of the *Charter*, must be interpreted purposively, that is to say, to further the interests it was intended to protect. . . . A privacy interest worthy of protection is one the citizen subjectively believes ought to be respected by government and "that society" is prepared to recognize as "reasonable."[5]

8. At no point did the Court of Appeal for Newfoundland consider, normatively, what the scope of the private sphere should be over the long-term, given the recognized importance of a robust concept of privacy to individual self-expression, democracy, and freedom.[6] The normative approach asks the judge to examine not only what is, but also what ought to be.[7]

9. One-on-one digital communications can still have a high expectation of privacy, even where the co-conversant is a stranger. In *R. v. Spencer*, this Court recognized the concept of privacy as anonymity. It held that anonymity permits individuals to act in public places, like the internet, but to preserve freedom from identification and surveillance: "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public."[8]

---

[4] *R. v. Spencer*, [2014] 2 S.C.R. 212, at para. 18; *R. v. Gomboc*, [2010] 3 S.C.R. 211, at para. 34 per Deschamps J., at para. 115 per McLachlin C.J. and Fish J. (dissenting in the result); *R. v. Patrick*, [2009] 1 S.C.R. 579, at paras. 12, 14; *R v M (A),* [2008] 1 S.C.R. 569, at para. 33 per Binnie J.; *R. v. Tessling*, [2004] 3 S.C.R. 432, at para. 42

[5] *R. v. M(A), supra*, per Binnie J., writing for the majority on this point, at para. 33, quoting from the United States Supreme Court decision in *United States v. Katz*, 389 U.S. 347 (1967)

[6] *Hunter v. Southam Inc*, [1984] 2 S.C.R. 145; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wong*, [1990] 3 S.C.R. 36

[7] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford: Stanford University Press, 2010), at pp. 233-4

[8] *Spencer, supra*, at paras. 38-50

10. Whether participating anonymously or not, online spaces are important spaces for expressive and associational freedom.[9] This may especially be so when communicating with someone who the individual has never met face-to-face. Expectations of privacy in communications may be formed even amongst strangers as a result of their shared bond or beliefs. The subject matter of such expressive and associational activities may reveal information that the individual might never share even with their closest friends or family. The unfortunate success rate of online dating fraud alone strongly suggests that—rightly or wrongly—individuals *do* form relationships of trust with "strangers" online.[10]

11. For individuals communicating in a private conversation online, expressive and associational activity occurs within a "situational landscape," analogous to that considered in *R. v. Wise*.[11] In participating as one of an abundant mass of individuals on the Internet, individuals reasonably do not expect to be under the intensive gaze of the state. As La Forest J. wrote in *Wise*:

> In a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the "situational landscape." The ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom. Justice Douglas recognized the importance of this privacy value in a democratic society, commenting that free movement is as dangerous to a tyrant as free expression of ideas or the right of assembly and is, therefore, controlled in most countries.[12]

12. The fact that the police technique targets criminal communications does not answer the question of whether the state should be permitted to engage in this form of surveillance without any oversight. Even the content of conversation relating to criminal activity may reveal highly personal

---

[9] *Spencer, supra*, at para. 48 citing Doherty J.A.'s decision in *R. v. Ward*, 2012 ONCA 660, at para. 71: "Personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society."

[10] Global News, "Canadians lost $16.9M to romance scams in 2015, fraud specialist says," dated February 19, 2016

[11] *R. v. Wise*, [1992] 1 S.C.R. 527

[12] *Wise*, *supra*

information, and still meaningfully be expected to be private.[13] Moreover, it is "the ***potential*** for revealing private information"[14] that must be considered in determining whether an electronic conversation attracts a reasonable expectation of privacy. As La Forest J. wrote in *Duarte*, "the relevant question is not whether criminals must bear the risk of warrantless surveillance, but whether it should be imposed on all members of society."[15]

B. The continuum of control that spans both spoken and text-based electronic conversations

13. The reasoning of the Newfoundland Court of Appeal in the instant appeal rests in part on a technological distinction between text-based and spoken communications. The Court of Appeal held that Mr. Mills "lost control"[16] over his communications once he hit send. Other lower court jurisprudence similarly holds that neither s. 8 nor Part VI are engaged by online undercover operations involving text-based communications.[17] Many of these cases hold that, unlike the voice conversations at issue in *Duarte*, or typical wiretaps of telephone conversations, the sender of a text-based communication *chooses* to create a permanent record of his or her own volition.

14. CIPPIC submits that this is not correct. The analysis cannot properly be driven by whether a communication is typed or spoken. As recognized in *R. v. TELUS Communications Co.* and *Marakah*, electronic text messaging shares many hallmarks of a traditional spoken conversation.[18] Moreover, technological advances in communications platforms have also blurred the lines between the modes of communication.[19] In many text-based platforms, the sender maintains a level of control over whether the recipient gets to keep an enduring copy of the sent message:

---

[13] *R. v. Craig*, 2016 BCCA 154 at para. 141; *R. v. Pelucco*, 2015 BCCA 370, at para. 53
[14] *Marakah*, *supra* at paras. 31 and 48 per McLachlin C.J. [emphasis added]
[15] *Duarte*, *supra* at p. 52
[16] *Mills*, CA Decision, at para. 23
[17] See *R. v. Allen*, 2017 ONSC 1712; *R. v. Merritt*, 2017 ONSC 1648; *R. v. Ghotra*, [2015] OJ No 7253 (SCJ); *R. v. Graff*, 2015 ABQB 415. See *contra, R. v. Kwok*, [2008] O.J. No. 2414 (CJ).
[18] *R. v. TELUS Communications Co*., [2013] 2 S.C.R. 3, at para. 1 per Abella J.; *Marakah*, *supra*, at para. 87 per Rowe J.
[19] This technological development is relevant to the scope of s. 8 protection: "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development": *R. v. Wong*, *supra* at p. 44

i. As this Court highlighted in *R. v. Marakah*, even an individual sending traditional text messages (SMS) exercises control over the information: "by choosing to send a text message by way of a private medium to a designated person, Mr. Marakah was exercising control over the electronic conversation."[20]

ii. Dozens of communication platforms (such as "Snapchat") allow users to send "self-destructing" videos, images, and typed communications. The messages automatically disappear from the recipient's device.

iii. Numerous electronic messaging platforms allow the ***sender*** of a message to ***delete*** the sent message off of the recipient's device—even after it is read and received. Platforms of this kind include popular messaging mediums such as Twitter direct messages, Instagram direct messages, and WhatsApp text messages.

iv. Other records of electronic messages remain within the control of a sender who determines whether their online "profile" remains active. The sender retains control over the messages by retaining control over the existence of their online profile (as demonstrated in the instant appeal, where the police deleted the Facebook profile used in the investigation).[21]

v. Other Internet-based communications platforms allow the recipients of a message to retain a copy of a sent message as long as the web browser remains open, but as soon as the session is closed, the messages are 'gone.'

15. This range of control is an important factor supporting the objective reasonableness of an expectation of privacy in one-on-one electronic communications, even where they are text-based.[22] It is true that many text-based communication platforms enable a recipient of a message to make or save a copy of an electronic communication. This may be so even where the platform is specifically designed to reduce that risk. However, this Court has held that 'control' should not be assessed in a rigid manner when analyzing privacy expectations technologically advanced communication mediums.[23] In this regard, the spectrum of control generally associated with many types of text-based messaging is sufficient to rebut any categorical distinction between voice- and text- based communications such as that relied upon by the courts below to defeat privacy expectations in private communications unknowingly sent to an agent of the state.

16. The distinction between voice and text drawn by the courts below is further undermined when

---

[20] *Marakah*, *supra* at para. 45 per McLachlin C.J.
[21] Appellant's Factum, at para. 16
[22] *Marakah*, *supra*, at para. 38 per McLachlin C.J., and at paras. 117, 155 per Moldaver J.
[23] *Marakah*, *supra*, at para. 41

technological advancements in voice-based communications are examined. For example, spoken communications sent via Internet (called voice over internet protocol, or "VOIP communications", such as Skype and Google Talk) are transmitted in precisely the same data packets as other typed messages sent over the Internet. These "records" of spoken communications sent over the Internet can be easily saved or copied in a manner that is indistinguishable from the screen capture program, Snagit, used by police to create a permanent record of the emails exchanged in this case. For both typed and spoken communications, the only way to retain absolute control is not to communicate at all. CIPPIC submits that the recipient's ability to make a permanent record of a communication should not be normatively determinative of the scope of the privacy expectation. In *Duarte*, this Court rejected the constitutionality of warrantless participant surveillance, ***even despite the fact*** that individuals are aware that their interlocutor may easily make a recording of the conversation in the absence of state involvement. The ease of the potential creation of a permanent record did not drive the analysis.[24]

17. CIPPIC submits that finely drawn technological distinctions between communications platforms therefore should not ground principled and normative determinations of when a reasonable expectation of privacy is engaged or when a police interposition constitutes an intercept. Such an approach would fall short of the aspirational purposes of section 8 and would yield an extraordinarily complicated and unpredictable framework that would be very difficult to implement.[25] An imputed assumption that text-based electronic conversations will be systematically copied and stored by the state is discordant from technological reality and the daily lived experience of Canadians with online communication platforms. The error of the assumption that typed communications inevitably create a permanent record is even made evident in the present appeal, where the only remaining record at trial

[24] The one-party consent exception in Part VI remains lawful amongst civilians in Canada to date.
[25] Users also often move contemporaneously between *multiple* mediums in an electronic conversation. It would beggar the concept of reasonable expectation of privacy to hold that, for example, communications sent between the same two conversants in the same "conversation" via Snapchat were protected by s. 8, but their VOIP communications were not. Reasonable expectations of privacy must be content-driven and technologically neutral.

of the one-on-one communications at issue was that created by the Snagit application.

C. An unregulated discretion by the state to surreptitiously interject into private, electronic conversations that are meant to be received by another individual endangers a free society

18. CIPPIC takes the position that a law enforcement officer who interposes under a falsified identity in a private communication and creates a record of the conversation (including via use of screen capture programs) is engaging in an "intercept" within the meaning of Part VI of the *Criminal Code*.[26] As the majority held in *R. v. Jones*, "interception relates to actions by which a third party interjects itself into the communication process in real-time through technological means."[27] Through the manipulation of the technological platform, the surveillance technique at issue confounds the individual's expectation that their communication is being received by the intended recipient. In defining "private communication" under Part VI, Parliament chose to protect an individual's reasonable belief that the communication will not be listened to, recorded, or acquired "***by any person other than the person intended by the originator to receive it.***"[28] CIPPIC submits that the Court of Appeal erred in concluding here that the undercover officer was the intended recipient of the communication.[29] This interpretation is inconsistent with the fact that the law criminalizes sexual offences against children over a computer, even where the offender is actually speaking to an undercover officer: "Where it has been represented to the accused that the person with whom he or she is communicating by computer (the 'interlocutor') is underage, the accused is presumed to have believed that the interlocutor was in fact underage."[30]

19. Like the surveillance technique considered in *Duarte*, the police technique at issue in the instant appeal also engages the need for section 8 protection, even in the absence of a finding that Part VI applies. As demonstrated in *Duarte*, *Wise*, and *Wong*, section 8 asks "whether [a] technology has the capacity to facilitate broad and indiscriminate surveillance and whether it would raise the spectre

---

[26] *Criminal Code*, s. 183 and 184(1)
[27] *R. v. Jones*, [2017] 2 S.C.R. 696, at para. 72
[28] *Criminal Code*, s. 183
[29] *Mills*, CA Decision, at paras. 13-14
[30] *R. v. Levigne*, [2010] 2 S.C.R. 3 at para. 32. See *Criminal Code*, ss. 171.1 and 172.1

of a surveillance state if deployment was left to the unfettered discretion of the state."[31] CIPPIC submits that the right under s. 8 to be *secure* against unreasonable search and seizure prevents the state from exercising a completely unregulated discretion to impersonate fictitious or real identities online and record the electronic communications that follow.

20. This technique does not simply engage the question decided long ago of whether individuals in a free society must assume the risk that our interlocutor is a tattletale. No one disputes that we do. Rather, the technique poses the markedly different question of whether we must be left unknowing as to whether the state, in its sole discretion, has falsified *or taken over in real-time* the electronic communications platform of even our most trusted confidantes without their knowledge or consent. By exploiting society's reliance on a technological medium, the technique leaves individuals in a digital version of an Orwellian reality, where "[t]here was of course no way of knowing whether you were being watched at any given moment."[32]

21. To leave the technique of undercover operations in one-on-one electronic conversations unregulated would thus undermine the aspirational values protected by section 8 of the *Charter*. Section 8 is itself a "precursor"[33] to the exercise of other rights and fundamental freedoms protected by the *Charter*. The following passage by Alan Westin, writing about the early development of computers in 1967, demonstrates the damage to free expression that would flow from imputing an assumption that one's interlocutor may be an undercover state agent making records of the electronic conversation:

> The danger to privacy and to…liberties in this development was that individuals who knew that all this information was being collected and stored and lay readily available in machines would never be able to know when it would be used "against them" and for what purposes. This public awareness of potential use would lead to an "increase in behaviour 'for the record'" and less freedom of action and expression. People will be concerned not only with the fact that they are going "on

---

[31] Renee Pomerance, "Informational Privacy in the Digital Age," in B. Berger, E. Cunliffe, and J. Stribopoulos, eds., *To Ensure that Justice is Done: Essays in Memory of Marc Rosenberg* (Toronto: Thomson Reuters, 2017), at p. 188; *Duarte*, *supra*; *Wise*, *supra*; *Wong*, *supra*.
[32] George Orwell, *1984* (London: Secker & Warburg, 1949), at p. 5
[33] Renee Pomerance, "Informational Privacy in the Digital Age," in Benjamin Berger, Emma Cunliffe, and James Stribopoulos, eds., *To Ensure that Justice is Done: Essays in Memory of Marc Rosenberg* (Toronto: Thomson Reuters, 2017), at p. 183

> record," but also with how that record will "look" to those in authority who examine it. The whole purpose of privacy…is to allow for unguarded, experimental "release" behaviour of individuals, and this outlet is just what our dossier-computer system is threatening.[34]

22. Writing two decades later in *Duarte*, this Court recognized the bottoming effect that risk analysis would have for a free society if individuals are required to assume that the state might be listening and recording when communicating. La Forest J. wrote that applying the risk assumption doctrine to warrantless participant surveillance would "destroy all expectations of privacy."[35] In *Duarte*, the undercover informant was in a direct conversation with Mr. Duarte, surreptitiously recording the conversation. Here, the risk posed to expectations of privacy would only be greater if the police, at their sole discretion, were permitted to assume online identities of individuals who have not agreed to act as an informer, and to create permanent records of the private communications that follow. Parliament chose to define a private communication under Part VI by reference to the originator's *intended* audience. As concluded in *Marakah*, the risk that the state "may be listening in and making a permanent record of the conversation…is not one that individuals should reasonably be required to bear."[36]

PART IV. SUBMISSIONS ON COSTS

23. CIPPIC does not seek costs and asks that no costs be awarded against it.

PART V. ORDER REQUESTED

24. CIPPIC makes no submission on the ultimate order to be made.

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

Jill Presser
Counsel to the Intervener, CIPPIC

Kate Robertson
Counsel to the Intervener, CIPPIC

---

[34] Alan Westin, *Privacy and Freedom* (New York: Simon & Schuster, Inc., 1967) at p. 349
[35] *Duarte*, *supra* at p. 48
[36] *Marakah*, *supra* at para. 127 per McLachlin C.J., citing *Duarte*, *supra* at p. 48-49

TABLE OF AUTHORITIES

Authority		Reference in Argument
	Cases	**Para**
1	*Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145	8
2	*R. v. Allen*, 2017 ONSC 1712	13
3	*R. v. Craig*, 2016 BCCA 154	12
4	*R. v. Duarte*, [1990] 1 S.C.R. 30	8, 12-13, 16, 19, 22
5	*R. v. Finlay* (1985), 23 C.C.C. (3d) 48 (Ont. C.A.)	1
6	*R. v. Ghotra*, [2015] OJ No 7253 (SCJ)	13
7	*R. v. Gomboc*, [2010] 3 S.C.R. 211	7
8	*R. v. Graff*, 2015 ABQB 415	13
9	*R. v. Jones*, [2017] 2 S.C.R. 696	1, 18
10	*R. v. Kwok*, [2008] O.J. No. 2414 (CJ)	13
11	*R. v. Levigne*, [2010] 2 S.C.R. 3	18
12	*R. v. M (A),* [2008] 1 S.C.R. 569	7
13	*R. v. Marakah*, [2017] 2 S.C.R. 608	2, 6, 12, 14-15, 22
14	*R. v. Merritt*, 2017 ONSC 1648	13
15	*R. v. Mills*, 2017 NLCA 12	3, 13, 18
16	*R. v. Patrick*, [2009] 1 S.C.R. 579	7
17	*R. v. Pelucco*, 2015 BCCA 370	12
18	*R. v. Spencer*, [2014] 2 S.C.R. 212	7, 9-10
19	*R. v. TELUS Communications Co.*, [2013] 2 S.C.R. 3	14
20	*R. v. Tessling*, [2004] 3 S.C.R. 432	7
21	*R. v. Ward*, 2012 ONCA 660	10
22	*R. v. Wise,* [1992] 1 SCR 527	11, 19

23	*R. v. Wong*, [1990] 3 S.C.R. 36	8, 14, 19
24	*United States v. Katz*, 389 U.S. 347 (1967)	7
	Additional Sources	
25	Alan Westin, *Privacy and Freedom* (New York: Simon & Schuster, Inc., 1967)	20
26	George Orwell, 1984 (London: Secker & Warburg, 1949)	20
27	Global News, "Canadians lost $16.9M to romance scams in 2015, fraud specialist says," dated February 19, 2016	10
28	Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford: Stanford University Press)	8
29	Renee Pomerance, "Informational Privacy in the Digital Age," in Benjamin Berger, Emma Cunliffe, and James Stribopoulos, eds., *To Ensure that Justice is Done: Essays in Memory of Marc Rosenberg* (Toronto: Thomson Reuters, 2017)	19, 21
	Legislation	
30	*Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK)*, 1982, c11, s. 8 / *La Charte Canadienne des droits et libertés, Partie I de la Loi constitutionnelle de 1982, Annexe B de la Loi de 1982 sur le Canada (R-U)*, 1982, c 11, s. 8	5, 7, 13-14, 17, 19, 21
31	*Criminal Code*, RSC 1985, c C-46, ss. 171.1-172.1 / *Code Criminel*, LRC (1985), ch C-46, ss. 171.1-172.1	18
32	*Criminal Code*, RSC 1985, c C-46, Part VI / *Code Criminel*, LRC (1985), ch C-46, Partie VI	5, 13, 16, 18-19
33	*Criminal Code*, RSC 1985, c C-46, ss. 183-184(1) / *Code Criminel*, LRC (1985), ch C-46, ss. 183-184(1)	18