Court File No. 34644

IN THE SUPREME COURT OF CANADA
(On Appeal from the Court of Appeal for Saskatchewan)

BETWEEN:

MATTHEW DAVID SPENCER

Appellant

-and-

HER MAJESTY THE QUEEN

Respondent

-and-

ATTORNEY GENERAL FOR ONTARIO, DIRECTOR OF PUBLIC PROSECUTIONS, ATTORNEY GENERAL FOR ALBERTA, PRIVACY COMMISSIONER OF CANADA, CANADIAN CIVIL LIBERTIES ASSOCIATION and CRIMINAL LAWYERS' ASSOCIATION OF ONTARIO

Interveners

FACTUM OF THE INTERVENER ATTORNEY GENERAL FOR ONTARIO

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

Allison Dellandrea
Susan Magotiaux

Tel.: 416-326-4600
Fax: 416-326-4656

Allison.Dellandrea@ontario.ca
Susan.Magotiaux@ontario.ca

Counsel for the Intervener
Attorney General for Ontario

Burke-Robertson LLP
Barristers and Solicitors
441 MacLaren Street
Suite 200
Ottawa, Ontario
K2P 2H3

Robert E. Houston, Q.C.

Tel.: 613-236-9665
Fax: 613-235-4430

rhouston@burkerobertson.com

Ottawa Agent for the Intervener
Attorney General for Ontario

McDougall Gauley LLP
1500-1881 Scarth Street
Regina, Saskatchewan
S4P 4K9

Aaron A. Fox, Q.C.
Darren K. Kraushaar

Tel.: 306-565-5147
Fax: 306-359-0785
afox@mcdougallgauley.co

Counsel for the Appellant
Matthew David Spencer

McMillan LLP
300-50 O'Connor Street
Ottawa, Ontario
K1P 6L2

Jeffrey Beedell

Tel.: 613-232-7171
Fax: 613-231-3191
jeff.beedell@mcmillan.ca

Agent for the Appellant
Matthew David Spencer

Attorney General for Saskatchewan
1874 Scarth Street, 3rd Floor
Regina, Saskatchewan
S4P 4B3

Anthony B. Gerein

Tel.: 306-787-5490
Fax: 306-787-8878
tony.gerein@gov.sk.ca

Counsel for the Respondent
Her Majesty the Queen

Gowling Lafleur Henderson LLP
2600-160 Elgin Street
P.O. Box 466, Station "D"
Ottawa, Ontario
K1P 1C3

Henry S. Brown, Q.C.

Tel.: 613-233-1781
Fax: 613-788-3433
henry.brown@gowlings.com

Agent for the Respondent
Her Majesty the Queen

Attorney General for Alberta
3rd Floor, Centrium Place
300, 332 – 6 Avenue S.W.
Calgary, Alberta
T2P 0B2

Jolaine Antonio

Tel.: 403-592-4902
Fax: 403-297-3453
jolaine.antonio@gov.ab.ca

Counsel for the Intervener
Attorney General for Alberta

Gowling Lafleur Henderson LLP
2600-160 Elgin Street
P.O. Box 466, Station "D"
Ottawa, Ontario
K1P 1C3

Brian A. Crane, Q.C.

Tel.: 613-233-1781
Fax.: 613-563-9869
brian.crane@gowlings.com

Agent for the Intervener
Attorney General for Alberta

Public Prosecution Service of Canada
700 EPCOR Tower 10423, 101st Street
Edmonton, Alberta
T4H 0E7

Ronald C. Reimer

Tel.: 780-495-4079
Fax.: 780-495-6940
ron.reimer@ppsc-sppc.gc.ca

Counsel for the Intervener
Director of Public Prosecutions

Director of Public Prosecutions of Canada
284 Wellington Street, 2nd Floor
Ottawa, Ontario
K1A 0H8

François Lacasse

Tel.: 613-957-4770
Fax.: 613-941-7865
flacasse@ppsc-sppc.gc.ca

Ottawa Agent for the Intervener
Director of Public Prosecutions

Kapoor Barristers
210-20 Adelaide Street East
Toronto, Ontario
M5C 2T6

James Stribopoulos

Tel.: 416-363-2700
Fax.: 416-368-6811
jst@kapoorbarristers.com

Counsel for the Intervener
Canadian Civil Liberties Association

Greenspon, Brown & Associates
331 Somerset Street West
Ottawa, Ontario
K2P 0J8

Lawrence Greenspon

Tel.: 613-288-2890
Fax.: 613-288-2896
email@lgreenspon.com

Ottawa Agent for the Intervener
Canadian Civil Liberties Association

Schreck Presser LLP
6 Adelaide Street East
5th Floor
Toronto, Ontario
M5C 1H6

Jill R. Presser
Jonathan Dawe

Tel.: 416-586-0330
Fax.: 416-977-8513
presser@schreckpresser.com

Counsel for the Intervener
Criminal Lawyers' Association of Ontario

Supreme Advocacy LLP
397 Gladstone Avenue
Suite 100
Ottawa, Ontario
K2P 0Y9

Marie-France Major

Tel.: 613-695-8855 ext. 102
Fax.: 613-695-8580
mfmajor@supremeadvocacy.ca

Agent for the Intervener
Criminal Lawyers' Association of Ontario

Osler, Hoskin & Harcourt LLP
1 First Canadian Place
P.O. Box 50
Toronto, Ontario
M5X 1B8

Mahmud Jamal

Tel.: 416-862-6764
Fax.: 416-862-6764
mjamal@osler.com

Counsel for the Intervener
Privacy Commissioner of Canada

Privacy Commissioner of Canada
Legal Services, Policy and Research Branch
Place de Ville, Tower B
112 Kent Street, 3rd Floor
Ottawa, Ontario
K1A 1H3

Patricia Kosseim
Daniel Caron
Sarah Speevak

Tel.: 613-947-4634
Fax.: 613-947-4192
patrica.kosseim@priv.gc.ca
daniel.caron@priv.gc.ca
sarah.speevak@priv.gc.ca

Agent for the Intervener
Privacy Commissioner of Canada

PART I: STATEMENT OF FACTS

1. When a bank account is allegedly used to launder proceeds of crime, the bank may give police a name and account number to aid in criminal investigation.[1]

2. When a rental car is seen participating in a drug deal, the rental company can give police the rental contract and driver's name and address to allow follow-up.[2]

3. When a cell number is associated to a call placed from a murder scene, moments before the death, police may ask for and receive subscriber information from the phone company so that they may seek judicial authorization to get content records.[3]

4. And when a computer broadcasts its "address" as a place to which the public is invited to share materials, an Internet Service Provider (ISP) who rented out that "address," at that point in time, may tell police the name and address of the client who is linked to the use of the service. When the files on offer are images of child abuse, the public expects no less.

5. An individual retains protection for intimate details at the point at which police seek to access those details. In this case, the details the police requested from Shaw Communications were a name and an address connected to an Internet Protocol (IP) address associated to child pornography at one point in time. Like the bank, the car rental shop, and the telephone company, the ISP decided to produce the subscriber information.

6. Under the direction of this Court's strong line of cases from *R. v. Plant* to *R. v. Cole*, the proper analysis of the s. 8 claim should focus on the nature of the information actually obtained, and the details that it alone provides. The sheet faxed by Shaw Communications[4] did not reveal information tending to expose the appellant's intimate biographical details: it did not identify the appellant at all. That should end the matter.

7. The Attorney General for Ontario takes no position on the facts of this case.

---

[1] *R. v. James*, [2013] O.J. No. 3591 (S.C.J.).
[2] *R. v. Siemens*, [2011] S.J. No. 406 (P.C.).
[3] *R. v. Pervez*, [2005] A.J. No. 708 (C.A.).
[4] Shaw Response, Appellant's Record, p. 127.

PART II: POINTS IN ISSUE

8. The Attorney General for Ontario supports the position of the respondent that there is no reasonable expectation of privacy in subscriber information and advances three points in this appeal:

i. Privacy interests in information are assessed only in relation to the nature of the information actually obtained by police. The privacy interest in information is **not** assessed by what police may learn by combining it with information lawfully possessed before or lawfully accessed later.

ii. In alleged Internet transmission of child pornography, as in banking, education, repair services and the like, unwitting third party conduits should be able to provide police with basic information to facilitate investigation.

iii. The *Personal Information Protection and Electronic Documents Act*[5] (*PIPEDA*) neither creates nor limits the authority of law enforcement. Nor does it grant s.8 privacy protection to individuals. *PIPEDA* is one factor that can assist in assessing the reasonableness of an individual's expectation that information in the hands of private entities will not be disclosed in particular circumstances.

PART III: BRIEF OF ARGUMENT

1. Maintaining Focus on the Nature of the Information

Clarity of Concepts: IP Address & Subscriber Data

9. Clarity of concepts is essential in this case. The evolving complexities of digital technology create a fruitful landscape for conceptual misunderstanding, fear and mistake. Such errors are evident in submissions of this case. The appellant says numerous times that what the police sought from Shaw was IP addresses and user information.[6] He is wrong. The Privacy Commissioner and Canadian Civil Liberties Association say that the combination of a subscriber name with a point-in-time IP address permits the police to see the surfing history, habits, predilections and even thoughts of an individual.[7] Not so.

10. The "search" or "seizure" that the appellant challenges is the transfer of

---

[5] S.C. 2000, c. 5, s. 3.
[6] Factum of the Appellant, paras. 73, 77 (IP address), paras. 27(2), 39 (user information).
[7] Factum of the Intervener Privacy Commissioner of Canada, paras. 17-20; Affidavit of Nathalie des Rosiers, Motion for Leave to Intervene, para. 20.

subscriber data only. Subscriber data includes the name and address of the Internet services customer. An IP and a subscriber account, even put together, tell the police nothing about who used a computer, or what else that device or user accessed in that session or on any other occasion. That is apparent on the facts of this case, where neither the subscriber information, nor the IP address said anything about Matthew David Spencer or his computer or his online travels. Police got that information only when executing a judicially authorized warrant.[8]

Clarity in Action: This Court's Direction on the Reasonable Expectation of Privacy

11. In *R. v. Plant*[9], *R. v. Edwards*[10], *R. v. Tessling*[11], *R. v. Patrick*[12] and *R. v. Gomboc*[13] this Court developed and refined a comprehensive and practical framework for assessing reasonable expectation of privacy in an informational context. That framework does not include consideration of prior police knowledge or the links that may be made in future stages of the investigation as a result of information obtained. In advancing the proposition that the appellant' s reasonable expectation of privacy should be assessed with respect to what else police observed publically on the Internet or learned after a judicially authorized home search, the appellant asks this Court to change the law and undermine years of consistent s.8 jurisprudence. The Attorney General for Ontario cautions against such an unworkable and unwarranted expansion of concepts of privacy.

12. Using the guidance of this Court, lower courts have overwhelmingly found no reasonable expectation of privacy in ISP held subscriber information.[14] Ontario adopts

---

[8] Appellant's Record, p. 92.
[9] [1993] 3 S.C.R. 281 at 293.
[10] [1996] 1 S.C.R. 128.
[11] [2004] 3 S.C.R. 432.
[12] [2009] 1 S.C.R. 579.
[13] [2010] 3 S.C.R. 211.
[14] *R. v. Ward,* [2012] O.J. No. 4587 (C.A.); *R. v. Connor,* [2009] O.J. No. 6390 (S.C.J.); overturning *Re. (S.C.),* [2006] O.J. No. 3754 (C.J.); *R. v. Vasic,* [2009] O.J. No. 685 (S.C.J.); *R. v. Friers,* [2009] O.J. No. 1080 (C.J.); *R. v. Verge,* [2009] O.J. No. 6300 (C.J.); *R. v. McGarvie,* [2009] O.J. No. 6417 (C.J.); *R. v. Wilson,* [2009] O.J. No. 1067 (S.C.J.); *R. v. Ewanyshyn,* (unreported), March 29, 2009 (Alta. Q.B.); *R. v. McNeice,* [2010] B.C.J. No. 2131 (S.C.); *R. v. Lo,* [2011] O.J. No. 4897 (S.C.J.); *R. v. Brousseau,* [2010] O.J. No. 5793 (S.C.J.); Contra: *R. v. Kwok,* [2008] O.J. No. 2414 (C.J.). *Kwok* was distinguished by the Ontario Court of Appeal in *R. v. Ward, supra,* on the basis that the *Kwok* court did not have a full record of the existence and detail of the contract governing use of information held by the commercial third party.

and recommends Ottenbreit J.A.'s analysis of this issue in the Court of Appeal:[15]

> In my view the disclosed information in this case merely establishes the identity of the contractual user of the IP address, who in this case was not the accused. The potential that the Disclosed Information might in this case eventually reveal much about the individual and the individual's activity is, in my view, neither here nor there. In my respectful view, the fact that the Disclosed Information is of such a quality that it is capable of being used to assist in obtaining a search warrant which will lead to revealing to the police more intimate details about the person once the warrant is granted and executed, does not take it beyond what it is at this stage – simply name, address and telephone number. Theoretically, all the assertions in an information to obtain a search warrant have the potential of revealing to the police more intimate details of a person once the search warrant is granted and executed. In this respect the Disclosed Information has, in my view, no different special quality than any other piece of information that they police may receive prior to the warrant which furthers the investigation. [Emphasis added].

Argument by Analogy

13. Stepping back from the computer context, this Court's jurisprudence on the definition of reasonable expectation of privacy provides a solid foundation for the continued focus of s.8 analysis on what information the police actually get, not what else they may piece together. In *Plant*, this Court framed the analysis with consideration of the nature of the information obtained by police, specifically, whether the information tended to reveal intimate details or intrude on the biographical core.[16] Hydro records, although they pertained to a residence, and were sought as a link in the chain to identify a criminal perpetrator, did not, in themselves, reveal intimate details. The same focus, and the same result are found in *Gomboc*. Again, Justice Deschamps, for the majority, emphasized that the device that monitored home electricity use could produce no intimate details, and would only support reasonable grounds to believe a grow-op was present when it was combined with information police had obtained from other sources.[17] Again, the s. 8 inquiry was shaped by information actually obtained in the impugned search, not the sum total of what police learned or could learn from its combination with other investigative fruits.

---

[15] *R. v. Spencer,* [2011] S.J. No. 729 at paras. 109-111 (C.A.). Ottenbreit J.A. offers a more comprehensive explanation of this analysis in *R. v. Trapp,* [2011] S.J. No. 728 at paras. 90-117, 134-135 (C.A.).
[16] *R. v. Plant, supra* at 293.
[17] *R. v. Gomboc, supra* at paras. 38, 47-48, 50.

14. In *Tessling*, the unanimous Court expressly narrowed the s. 8 analysis to "the quality of information that the FLIR imaging can actually deliver", not it's "theoretical capacity".[18] Since the information produced by the FLIR machine, considered in isolation, was meaningless, no reasonable expectation of privacy was found.[19] Similarly, fearful musings about the potential technological capabilities of law enforcement were quieted with a firm focus on the technology known and used in the instant case, as set out in the evidentiary record before the Court. *Tessling* teaches that important constitutional issues involving technology must be considered on the basis of fact, not speculation of future fruitfulness.[20]

15. This Court's guidance has been well used. Lower courts continue to apply the totality of circumstances test with a focus on the information actually obtained, not the overall inferences police seek to support or the theoretical capability of police techniques. Bank account subscriber names and addresses,[21] rental car contracts,[22] passenger lists,[23] and mail box rental logs[24] do not reveal intimate details. They do not identify historical peregrinations. Nor do subscriber details of telephone services.[25] This is so even though it is possible that a phone number or bank account or IP address could be linked to some historical activity or community involvement through publically available means. The potential to link information is not new, is not unique to the computer context, and does not alter the s. 8 analysis.

16. The totality of circumstances approach developed by this Court should not be altered; and certainly not by reference to facts which are speculative, unknown, or untrue.

---

[18] *R. v. Tessling, supra* at paras. 28-29.
[19] *R. v. Tessling, supra* at para. 58. See also paras. 34-35, 62-63.
[20] *R. v. Tessling, supra* at paras. 34-36, 55; *R. v. Gomboc, supra* at para. 40.
[21] *R. v. Lillico* (1994), 92 C.C.C. (3d) 90 at paras. 6-7, 12-13 (Ont. Gen. Div.); upheld [1999] O.J. No. 95 at para. 3 (C.A.); *R. v. Quinn* (2006), 209 C.C.C. (3d) 278 at paras. 82-92 (B.C.C.A.); *R. v. James, supra* at para. 64.
[22] *R. v. Siemens, supra* at paras. 51-54.
[23] *R. v. Chehil,* [2009] N.S.J. No. 515 at paras. 34-57 (C.A.); *R. v. Tan,* [2010] B.C.J. No. 2803 at paras. 22-31 (S.C.).
[24] *R. v. Stucky,* [2006] O.J. No. 108 (S.C.J.).
[25] *R. v. Brown,* [2000] O.J. No. 1177 at paras. 30-33, 63-66 (S.C.J.); *R. v. Edwards,* [1999] O.J. No. 3819 at paras. 33-39 (S.C.J.); *R. v. Hutchings* (1996), 111 C.C.C. (3d) 125 at paras. 22-25 (B.C.C.A.); *R. v. Pervez, supra* at paras. 7-14. Contra: *R. v. Nguyen,* [2004] B.C.J. No. 248 at paras. 20-25 (S.C.), but see *R. v. Pal,* [2007] B.C.J. No. 2193 at paras. 21-27 (S.C.).

2. THE SILENT PARTNER?: THIRD PARTY CONDUITS OF CRIME

17. Where a third party finds itself the unwitting conduit or victim of criminal conduct, s. 8 of the *Charter* cannot operate to compel its silence. It would be a strange result if the third party was paralyzed from making disclosure of its own victimization or complicity based on the private nature of the information related to the use of their services for a criminal purpose. The unwilling facilitator should be able to provide information to the police so that a proper investigation may occur to protect the public from further offending, and to protect its own interests.

18. Shaw clearly expressed its interest in disassociating itself from any criminal use of its services, and reporting such uses, in its *Joint Terms of Service* and *Unacceptable Use Policy* documents which indicate that:

a. Transmission of child pornography equals a breach of contract;
b. Shaw may monitor content and has the right to disclose 'illegal activity';
c. Shaw "may cooperate with law enforcement in the investigation of suspected criminal violations by providing the username, IP address, or other identifying information about the subscriber, in accordance with the guidelines set out in Shaw's privacy policy"

19. Irrespective of its terms of service, Shaw's right to provide tombstone data to the police should also flow from recognition of its status as a conduit of crime. Shaw's own interest in avoiding potential liability for the transmission of child pornography over its services is real and legitimate.[26] Just as with other institutional contexts such as banking, utilities, education and repair services, ISPs which are unwitting conduits or victims of criminal conduct must have the right to report basic information to the police to facilitate the investigation of crime.

20. If Shaw had discovered that IP 70.64.12.102 at 12:46 on August 31, 2007 had transmitted child pornography on its own, it could without a doubt have reported this information, together with the associated subscriber information to the police: both to protect its own interests, and out of civic duty. In *Gomboc*, this Court affirmed the

---

[26] *R. v. Ward, supra* at paras. 97-100.

importance of "voluntary cooperation of a potential crime victim": [27]

> ... if the police had merely notified Enmax of a potential electricity theft and the utility had proceeded on its own initiative to install a DRA and turn over what it disclosed, no *Charter* violation would have arisen. Only by misguidedly elevating form over substance would a contrary conclusion result solely because Enmax installed a DRA subsequent to a police request for cooperation. [Emphasis added].

21. Voluntary third party disclosure has been considered in the specific context of ISPs as "conduits" of crime. In *R. v. Friers*, the Court held that where Internet service providers report concerns about the illegal use of their services, there should be "no difficulty" in finding that the subscriber does not have a reasonable expectation of privacy in the customer information provided to the police.[28]

22. In *R. v. Cole*, this Court confirmed that a school board was legally entitled to inform the police of its discovery of contraband on an employee's laptop, thereby permitting the police the opportunity to seek a search warrant to access the computer's content.[29] The school board's reporting of their discovery was presumably motivated by their desire to disassociate from the criminal conduct (facilitated by their equipment), as well as by their sense of civic duty.

23. Computer repair persons who discover the existence of child pornography on a device – and unwittingly become the custodians of contraband – may, like the school board, report the discovery to police without offending s. 8 of the *Charter*.[30] Just as in the ISP context, a search warrant is required in such cases for the subsequent search and seizure of the computer itself.

24. Similar conclusions have been reached in a variety of commercial contexts, where the customer's right to confidentiality has yielded to the public's right to effective law enforcement through the voluntary disclosure of certain of their information held by

---

[27] *R. v. Gomboc, supra* at para 42.
[28] *R. v. Friers, supra* at para. 21.
[29] *R. v. Cole,* [2012] 3 SCR 34 at para. 73.
[30] *R. v. Winchester,* [2010] O.J. No. 281 at paras. 50-53 (S.C.J.).

its custodians.

- Banks are permitted to disclose evidence of fraud to the police. They do not need to "sit, silent, and hope an external investigator persists with a search warrant or court order to disclose documents."[31]

- Utility companies whose services are being stolen or misused are potential crime victims who are entitled to voluntarily disclose customer data in order protect their own interests.[32]

- Car rental companies can provide police with vehicle rental information when their vehicles are believed to have been used in the trafficking of narcotics. [33]

25. The reasoning expressed in these cases is directly applicable on this appeal. Detective Sergeant Parisien sent a letter of request to Shaw advising them that an IP Address belonging to their service had been associated with the distribution of child pornography.[34] Upon receiving this information, Shaw was in the same position as the school board in *Cole*, the banks in *R. v. Lillico, R. v. James,* and *R. v. La*, the utility company in *Gomboc*, and the repair shop in *R. v. Winchester*: it was possessed of information that it's services had unwittingly been used for suspected criminal conduct, in this case, the sharing of child abuse images. ISPs must surely enjoy the same right to distance themselves from such conduct and to assist in the identification of perpetrators as would any other company or citizen.

3. *THE LIMITED ROLE OF* PIPEDA

26. The Privacy Commissioner argues that *PIPEDA* does not diminish privacy and that s. 7(3)(c.1)(ii) does not authorize police to intrude on reasonable expectations of privacy.[35] She is right on both points. No one is arguing otherwise.

27. Contracts and statutes governing the use and disclosure of information in commercial relationships have always played a role in the s. 8 analysis. That role is important, but limited. A federal statute enacted "to support and promote electronic

---

[31] *R. v. La,* [2012] A.J. No. 332 at para. 55 (Q.B.); *R. v. James*, *supra* at para. 64; *R. v. Lillico*, *supra.*
[32] *R. v. Gomboc, supra* at para. 42.
[33] *R. v. Siemens*, *supra* at paras. 16, 57.
[34] Law Enforcement Request and Reply, Appellant's Record, p. 123.
[35] Factum of the Privacy Commissioner of Canada, paras. 3-4.

commerce"[36] does not and cannot redefine the constitutional standard in s. 8 of the *Charter* or increase the scope of information that is protected from state intrusion.[37]

28. In certain situations, *PIPEDA* explicitly permits information held by a private entity to be shared with law enforcement without the knowledge or consent of the person to whom the information relates. Section 7(3) governs disclosure pursuant to court order or warrant. Section 7(3)(c.1), in contrast, recognizes the discretion of commercial entities to disclose information to law enforcement absent a court order or warrant. *PIPEDA* places individuals on notice that the third party private entity who is in possession of their information can disclose it to a police officer who requests the information "for the purpose of enforcing any law of Canada ... [or for] carrying out an investigation relating to the enforcement of any such law ...".

29. While s. 7(3)(c.1)(ii) contemplates and permits sharing of information in response to government requests, it does not require disclosure to law enforcement. Suggestion by the Appellant that ISPs are forced to submit by the strong arm of the state are unsupported.[38] In fact, many ISPs collaborated with law enforcement to develop a protocol for dealing with requests for subscriber information.[39] In child exploitation investigations, the protocol provides that a participating ISP, in response to an agreed upon form of request letter, will disclose to police the last known name and address of the account holder that was using a particular IP address at a specific date and time.

30. If information in the hands of a third party is s. 8 *Charter* protected, because it engages a reasonable expectation of privacy, then regardless of whether the third party is willing to provide that information to police or not, barring exigent circumstances or some other warrantless search doctrine, *Hunter v. Southam* demands judicial authorization.[40] Whether or not a person has a reasonable expectation of privacy that

---

[36] House of Commons Debates, No. 9 (22 October 1999) at 1005.
[37] *R .v. Chehil, supra,* at paras. 23-24.
[38] Appellant's Factum, paras. 77-81; *R. v. Brousseau, supra,* at paras. 42-45.
[39] Suzanne Morin, "Updated: Business Disclosure of personal information to law enforcement agencies: PIPEDA and the CNA letter of request protocol" (2011) CBA National and Privacy Access Law Section Newsletter at p. 1.
[40] *Hunter v. Southam Inc.,* [1984] 2 S.C.R. 145; *R. v. Plant, supra* at 294; *R. v. Wilson, supra* at para. 39; *R. v. Brousseau, supra* at paras. 41-45; *R. v. Chehil, supra* at para. 29.

attracts s. 8 protections is assessed under the totality of circumstances test and is focused on the content of the information.

31. *PIPEDA* and the Office of the Privacy Commissioner play important roles in the protection of privacy in commercial dissemination of information. In the criminal sphere, state access to information has always been governed by the constitutional demands of s. 8, as interpreted by this and other courts. Under the *Patrick* analysis of totality of circumstances, there is room for consideration of the rules and regulations governing third party use of information provided by an individual.[41] *PIPEDA* is only one rung in the ladder of totality. It should not shape or reshape the s. 8 lens.

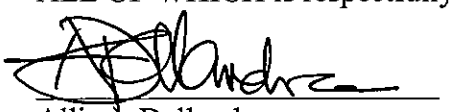
PART IV: SUBMISSIONS ON COSTS

32. The Attorney General for Ontario makes no submissions as to costs.

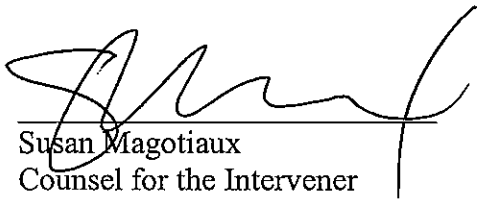
PART V: ORDER REQUESTED

33. The Attorney General for Ontario respectfully requests the appeal be dismissed and requests that an Order be made permitting it to present 10 minutes of oral argument at the hearing of the appeal.

ALL OF WHICH is respectfully submitted by



Allison Dellandrea
Counsel for the Intervener
Attorney General for Ontario



Susan Magotiaux
Counsel for the Intervener
Attorney General for Ontario

DATED this 25th day of September, 2013

[41] See also *R. v. Gomboc, supra,* at para. 32; *R. v. Cole, supra,* at para. 3; *R. v. McNeice, supra,* at para. 50; *R. v. Vasic, supra,* at para. 54-55; *R. v. Wilson, supra,* at paras. 41-43; *R. v. Lo, supra,* at paras. 42-47.

PART VI: TABLE OF AUTHORITIES