

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

B E T W E E N:

MATTHEW DAVID SPENCER

Appellant

- and -

HER MAJESTY THE QUEEN

Respondent

- and -

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

Interveners

FACTUM OF THE INTERVENER,
PRIVACY COMMISSIONER OF CANADA

MAHMUD JAMAL

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

Tel: (416) 862-6764

Fax: (416) 862-6764

Email: mjamal@osler.com

Counsel for the Intervener,
Privacy Commissioner of Canada

PATRICIA KOSSEIM

DANIEL CARON

SARAH SPEEVAK

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

Tel: (613) 947-4634

Fax: (613) 947-4192

Email: patricia.kosseim@priv.gc.ca
daniel.caron@priv.gc.ca
sarah.speevak@priv.gc.ca

Counsel for the Intervener,
Privacy Commissioner of Canada

ORIGINAL: **The Registrar**
The Supreme Court of Canada
301 Wellington Street
Ottawa, Ontario K1A 0J1

Tel: (613) 995-4330
Fax: (613) 996-3063
Email: reception@scc-csc.gc.ca

COPY TO:

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
E-mail: afox@mcdougallgauley.co

Counsel for the Appellant,
Matthew David Spencer

McMillan LLP
Suite 300, 50 O'Connor Street
Ottawa, ON K1P 6L2

Jeffrey Beedell

Tel: (613) 232-7171
Fax: (613) 231-3191
E-mail: jeff.beedell@mcmillan.ca

Agent for the Appellant,
Matthew David Spencer

AND TO:

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

Anthony B. Gerein

Tel: (306) 787-5490
Fax: (306) 787-8878
E-mail: tony.gerein@gov.sk.ca

Counsel for the Respondent,
Her Majesty the Queen

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

Henry S. Brown, Q.C.

Tel: (613) 233-1781
Fax: (613) 788-3433
E-mail: henry.brown@gowlings.com

Agent for the Respondent,
Her Majesty the Queen

Attorney General of 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
E-mail: jolaine.antonio@gov.ab.ca

**Counsel for the Intervener,
Attorney General of 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
E-mail: ron.reimer@ppsc-sppc.gc.ca

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

Attorney General of Ontario

720 Bay St
10th Floor
Toronto, Ontario M5G 2K1

Michal Fairburn

Tel: (416) 326-4658
Fax: (416) 326-4656
E-mail: michal.fairburn@ontario.ca

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

Gowling Lafleur Henderson LLP

2600 - 160 Elgin St
Box 466 Station D
Ottawa, Ontario K1P 1C3

Brian A. Crane, Q.C.

Tel: (613) 233-1781
Fax: (613) 563-9869
E-mail: brian.crane@gowlings.com

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

**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
E-mail: flacasse@ppsc-sppc.gc.ca

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

Burke-Robertson

441 MacLaren Street
Suite 200
Ottawa, Ontario K2P 2H3

Robert E. Houston, Q.C.

Tel: (613) 236-9665
Fax: (613) 235-4430
E-mail: rhouston@burkerobertson.com

**Agent for the Intervener,
Attorney General of Ontario**

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

James Stribopoulos

Tel: (416) 363-2700
Fax: (416) 368-6811
E-mail: jst@kapoorbarristers.com

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

Dawe Dineen
171 John Street, Suite 101
Toronto, Ontario M5T 1X3

Jonathan Dawe

Tel: (416) 649-5058
Fax: (416) 352-7733
Email: jdawe@dawedineen.com

Schreck Presser LLP
5th Flr., 6 Adelaide St. E.
Toronto, Ontario M5C 1H6

Jill Presser
Tel: (416) 586-0330
Fax: (416) 977-8513
E-mail: presser@schreckpresser.com

**Counsel for the Intervener,
Criminal Lawyers' Association of
Ontario**

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

Lawrence Greenspon

Tel: (613) 288-2890
Fax: (613) 288-2896
E-mail: email@lgreenspon.com

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

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
E-mail: mfmajor@supremeadvocacy.ca

**Agent for the Intervener,
Criminal Lawyers' Association of
Ontario**

TABLE OF CONTENTS

PART I – OVERVIEW	1
PART II – ARGUMENT	2
1. <i>PIPEDA</i> Protects Rather than Diminishes Privacy Rights	2
2. Section 7(3)(c.1)(ii) of <i>PIPEDA</i> Does Not Authorize The Police To Intrude on a Reasonable Expectation of Privacy	3
3. Subscriber Information is a Potential “Gateway” to Core Biographical Information	5
4. Standard Terms in a Commercial Adhesion Contract Do Not Eviscerate or Dilute Privacy Rights Against the State; Nor Do They End the Privacy Analysis Under <i>PIPEDA</i>	7
5. The Seriousness of Child Pornography Offences Should Not Diminish The Reasonable Expectations of Privacy of Ordinary Canadians on the Internet	10
PART III – ORDER SOUGHT	11
PART IV – TABLE OF AUTHORITIES	12
PART V – TABLE OF STATUTES	15

PART I – OVERVIEW

1. A central issue in this appeal is whether ordinary Canadians have a reasonable expectation of privacy vis-à-vis the state in subscriber information held by their Internet service provider (“ISP”). Such information has the potential to identify them and reveal details of their online activities. Every device connected to the Internet is assigned a unique identifier by the ISP known as an “IP address” which, when linked to subscriber information, has the potential to reveal a vast amount of information about sites visited and documents downloaded not only by the subscriber, but also by other individuals sharing the subscriber’s Internet service. The critical privacy issues in this appeal arise in the context of a criminal prosecution involving possessing and making available child pornography, but have broader implications for the privacy expectations of all Canadians whenever they use the Internet, whether in their homes or elsewhere.

2. In this context, the Privacy Commissioner of Canada (“Privacy Commissioner”) has five points relating to the privacy issues raised by this appeal.

3. First, the courts below erred in finding that the provisions of the *Personal Information Protection and Electronic Documents Act*¹ (“PIPEDA”) weigh against the accused having a reasonable expectation of privacy in subscriber information held by an ISP. Properly interpreted in accordance with Parliament’s intent, *PIPEDA* protects rather than diminishes privacy rights. It is a privacy protection statute.

4. Second, s. 7(3)(c.1)(ii) of *PIPEDA* does not authorize the police to intrude on a reasonable expectation of privacy. This provision requires the police to identify an independent source of “lawful authority to obtain” ISP subscriber information; it does not itself grant that “lawful authority”. Where the police request intrudes on a reasonable expectation of privacy (as it did in this case), prior judicial authorization is still required.

5. Third, far from being inconsequential, subscriber information is “gateway information” that can provide the state with a detailed roadmap of an individual’s most intimate views, opinions, and activities online. Such information therefore deserves constitutional protection under s. 8 of the *Charter*.

¹ S.C. 2000, c. 5.

6. Fourth, a term in a subscriber's adhesion contract providing that an ISP may disclose personal information to police should have little if any weight in diminishing a person's reasonable expectation of privacy vis-à-vis the state.

7. Fifth, requests for subscriber information in the context of child pornography investigations should not be used to diminish the reasonable expectation of privacy of ordinary Canadians. The analysis under s. 8 of the *Charter* must be conducted in "broad and neutral terms," not skewed by the presence of serious allegations of criminality. The seriousness of the offence can, however, be evaluated in assessing the admissibility of any unconstitutionally obtained evidence under s. 24(2) of the *Charter*.

PART II – ARGUMENT

1. *PIPEDA* Protects Rather than Diminishes Privacy Rights

8. With respect, the courts below erred in finding that s. 7(3)(c.1)(ii) of *PIPEDA* weighs against an accused having a reasonable expectation of privacy in subscriber information held by an ISP.² Because the purpose of *PIPEDA* is to **protect** personal information, holding that *PIPEDA* is a factor that **reduces** an individual's expectation of privacy vis-à-vis the state is inconsistent with Parliament's intention.

9. *PIPEDA* is a privacy protection statute;³ the quasi-constitutional nature of the protection of personal information has been recognized by this Court and other courts on numerous occasions.⁴ In short, *PIPEDA* **protects** rather than **diminishes** individuals' privacy rights.

² *R. v. Spencer*, 2011 SKCA 144, ¶¶34-41; *R. v. Spencer*, 2009 SKQB 341, ¶19.

³ *Royal Bank of Canada v. Ren*, 2009 ONCA 48, ¶22.

⁴ *Pro Swing Inc. v. Elta Golf Inc.*, [2006] 2 S.C.R. 612, ¶60; *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 S.C.R. 441, ¶28; *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, ¶24; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, ¶¶65-66. See also *Nammo v. TransUnion of Canada Inc.*, 2010 FC 1284, ¶74 and *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070, ¶43.

2. Section 7(3)(c.1)(ii) of *PIPEDA* Does Not Authorize The Police To Intrude on a Reasonable Expectation of Privacy

10. One of the cornerstones of *PIPEDA* is the obligation to obtain the knowledge and consent of an individual to collect, use, or disclose their personal information. Parliament has expressly limited any non-consensual collection, use, or disclosure of personal information to only those circumstances set out under s. 7 of *PIPEDA*.⁵ One such limited and discretionary exception is s. 7(3)(c.1)(ii), which permits an organization subject to *PIPEDA* to disclose an individual's personal information without their knowledge or consent if the disclosure is made to a government institution that has made the request for the information; identified its lawful authority to obtain the information; and indicated that the information requested is for the purpose of law enforcement.

11. Section 7(3)(c.1)(ii) of *PIPEDA* does not provide an exception to the requirement that the state obtain prior judicial authorization to conduct a search or seizure in the context of a criminal investigation.⁶ Section 8 of the *Charter* stands as “a shield against unjustified intrusions on personal privacy.”⁷ If the information targeted by the police is protected by a reasonable expectation of privacy, acquisition of this information by the police would constitute a “search” or “seizure” for the purposes of s. 8 of the *Charter*, even if the state conduct is in no way coercive.⁸ Section 7(3)(c.1)(ii) requires the police to identify their “lawful authority *to obtain*” (“droit de *l’obtenir*”), but does not itself provide that authority. Where the conduct of the police intrudes on a reasonable expectation of privacy, they still require prior judicial authorization to obtain the information.

12. Further, as a matter of statutory interpretation, s. 7(3)(c.1)(ii) of *PIPEDA* does not authorize the police to intrude on constitutional privacy rights and must be presumed to

⁵ *Wansink v. TELUS Communications Inc.*, 2007 FCA 21, ¶21.

⁶ *R. v. Tse*, 2012 SCC 16, ¶16.

⁷ *R. v. Kang-Brown*, [2008] 1 S.C.R. 456, ¶8.

⁸ *R. v. Tessling*, [2004] 3 S.C.R. 432, ¶18; *R. v. Buhay*, [2003] 1 S.C.R. 631, ¶¶33-34; *R. v. Law*, [2002] 1 S.C.R. 227, ¶15; *R. v. Wise*, [1992] 1 S.C.R. 527, pp. 533, 538; *R. v. Evans*, [1996] 1 S.C.R. 8, ¶11; see also *R. v. Ward*, 2012 ONCA 660, ¶64.

have been enacted to comply with constitutional norms.⁹ The government was clear in introducing this provision before Parliament that it did not give law enforcement authorities any new powers.¹⁰ The provision merely serves as a shield to protect private-sector organizations from liability if they choose to disclose personal information in permissible circumstances; it is not a sword or new source of authority for the police or other law enforcement authorities to access personal information that is entrusted to private-sector organizations otherwise obliged to protect privacy.

13. A simple written request by a police officer, while appearing authoritative, is not “lawful authority to obtain” subscriber information within the meaning of s. 7(3)(c.1)(ii) of *PIPEDA*. Otherwise, law enforcement could simply “request” medical information, fingerprints, financial information, or other types of sensitive personal information commonly held by organizations subject to *PIPEDA*, and escape *Charter* scrutiny. Such an approach would make short shrift of the constitutional principle that the state cannot access constitutionally-protected information without prior judicial authorization in accordance with s. 8 of the *Charter*.

14. Moreover, reading s. 7(3)(c.1)(ii) of *PIPEDA* to permit the police to access constitutionally-protected information without accountability and transparency measures overseeing their conduct would also be constitutionally problematic.¹¹ Section 7(3)(c.1)(ii) provides for no notice to the affected person, no reporting to Parliament, no requirement for record-keeping, nor any restrictions on the secondary uses that can be made of the targeted information. This interpretation of s. 7(3)(c.1)(ii) would flout this Court’s caution against allowing privacy violations without appropriate safeguards and oversight.

15. Such an interpretation would also make s. 7(3)(c) of *PIPEDA* redundant. Section 7(3)(c) permits an organization to disclose personal information without an individual’s

⁹ Tse, above, note 6, ¶20.

¹⁰ House of Commons Debates, No. 9 (22 October 1999) at 1015 (Hon. John Manley). See also Stephanie Perrin, Heather H. Black, David H. Flaherty and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law Inc., 2001), pp. 75, 165; see also *Royal Bank of Canada*, above, note 3, ¶22 (s. 7(3)(d) of *PIPEDA* merely codified “the existing common law which permitted the sharing of such information in similar circumstances”).

¹¹ Tse, above, note 6, ¶¶79-93.

knowledge or consent where required to comply with a subpoena, warrant, or court order. If a simple request from law enforcement to disclose information voluntarily is sufficient to constitute “lawful authority” under s. 7(3)(c.1)(ii), there would have been no need for Parliament to address situations under s. 7(3)(c). This would have been subsumed under s. 7(3)(c.1)(ii) as well, rendering s. 7(3)(c) superfluous.

16. Finally, s. 487.014 of the *Criminal Code* states, “for greater certainty,” that no production order is required for the police to ask a person **not** otherwise prohibited from disclosing information to provide that information voluntarily. It does not provide police with unqualified “lawful authority **to obtain**” information or to intrude on a reasonable expectation of privacy. This provision has been described as stating “the self-evident”, reflected in the opening phrase “for greater certainty,” that “where a person is not prohibited by law from disclosing information, the police may request disclosure of that information without prior judicial authorization.”¹² Contrary to situations where police question individual witnesses at the scene of a crime or an accident, here, *PIPEDA* itself prohibits organizations from disclosing the targeted information unless the police identify their “lawful authority to obtain” it, such that s. 487.014 of the *Criminal Code* simply does not apply.

3. Subscriber Information is a Potential “Gateway” to Core Biographical Information

17. This Court has recognized that in fostering the underlying values of dignity, integrity, and individual autonomy, s. 8 of the *Charter* seeks to shield from dissemination to the state information that would “tend to reveal,” but not necessarily by itself constitute, intimate details of an individual’s lifestyle, activities, opinions, and personal choices.¹³ The taking of an individual’s blood sample without consent, for example, is constitutionally significant exactly because it allows the police to link to, or derive other information about, an identifiable individual.¹⁴

¹² *Ward*, above, note 8, ¶49.

¹³ *R. v. Cole*, [2012] 3 S.C.R. 34, ¶45, citing *R. v. Plant*, [1993] 3 S.C.R. 281, p. 293; see also *R. v. Patrick*, [2009] 2 S.C.R. 579, ¶¶30-31.

¹⁴ *R. v. Dyment*, [1988] 2 S.C.R. 417, p. 427.

18. Similarly, an individual's name and address, when connected to an IP address, can provide the essential link to a vast amount of highly personal information, including detailed information about the individual's Internet browsing history. While subscriber information on its face already reveals some information about the individual (for example, an address can reveal where a person lives, with whom and their socio-economic status), the police do not seek such information for only its intrinsic value. Rather, they seek it because it allows them to associate an identifiable individual with significant amounts of other, often highly sensitive, personal or private information regarding the individual's Internet usage.

19. Because of the latent power that subscriber information yields, it is fundamentally different from customer information obtained in other contexts. A name and address in the hands of an ISP are not simply two individual pieces of data in isolation; all information can be broken down into distinct little pieces that, on their own, reveal little or no biographical core data.¹⁵ However, pieces of seemingly innocuous information, when viewed in their entirety along with other available information, can paint a fairly accurate and complete picture of one's personal activities, views, opinions, and lifestyle.¹⁶ Subscriber information is thus the tip of the iceberg for the state to form a detailed picture of an individual's Internet browsing activity, which would tend to reveal a biographical core of personal information.¹⁷

20. Giving the police access to such gateway information without a warrant would give them the immediate capacity to "scrutinize [...] the electronic roadmap of your

¹⁵ J. McGill and I. Kerr, "Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in *Digital Enlightenment Yearbook 2012*, ed. J. Bus et al. (IOS press, 2012), 199-217, at pp. 212-216; T. Scassa, "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010), 7 C.J.L.T. 193, pp. 200-201.

¹⁶ *Patrick*, above, note 13, ¶¶30-31; *R. v. Mahmood*, [2008] O.J. No. 3922 (S.C.J.), ¶¶55-82; *R. v. MacInnis*, [2007] O.J. No. 2930 (S.C.J.), ¶¶31-65; *R. v. Vasic*, [2009] O.J. No. 685 (S.C.J.), ¶54; *C. (S.)*, *Re*, 2006 ONCJ 343.

¹⁷ D. Gilbert, I. Kerr and J. McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2007), 51 *Crim. L.Q.* 470, pp. 487-488; J.J. McIntyre, "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information," (2011) 60 *DePaul L. Rev.*, pp. 2-7; Scassa, above, note 15, pp. 200-201; Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada* (May 2013); *R. v. A.M.*, [2008] 1 S.C.R. 569, ¶68 (s. 8 protects information reasonably intended to be kept private even if not "biographical core" information).

cybernetic peregrinations, where you have been and what you appear to have seen on the Internet – generally by design, but sometimes by accident.”¹⁸

21. In view of the ubiquity and necessity of computers and the Internet, and the growing trend of Canadians to lead more and more of their personal and social lives online, any finding that Internet users have no reasonable expectation of privacy in subscriber information would have profound implications for individual privacy in the modern technological age.

4. Standard Terms in a Commercial Adhesion Contract Do Not Eviscerate or Dilute Privacy Rights Against the State; Nor Do They End the Privacy Analysis Under PIPEDA

22. The Court of Appeal also erred in finding that the accused had no reasonable expectation of privacy in the ISP subscriber information vis-à-vis the state based in part on the terms of the particular service agreement with the ISP.¹⁹ The Court’s approach would allow third parties (ISPs), through adhesion contracts, to require a waiver of fundamental privacy rights as a non-negotiable condition for accessing the Internet.

23. ISP service agreements are often lengthy, detailed adhesion contracts comprising multiple documents, often including a separate “difficult to understand” online privacy policy.²⁰ Such agreements should be given limited, if any, weight in determining whether an individual enjoys a reasonable expectation of privacy against the state. A necessary, conditional consent for purposes of an ISP subscription agreement “does not trump our reasonable expectation of privacy in the information to which access is afforded for such a limited and well-understood purpose. *When we subscribe for cable services, we do not surrender our expectation of privacy in respect of what we access on the Internet, what*

¹⁸ *R. v. Morelli*, [2010] 1 S.C.R. 253, ¶3; see also ¶¶104-106.

¹⁹ *R. v. Spencer*, 2011 SKCA 144, ¶33 (Caldwell J.A.); cf. ¶¶97-98 (Cameron J.A.)

²⁰ S. Braman and S. Roberts, “Advantage ISP: Terms of Service as Media Law” in *New Media Society* (2003) 5: 422-448 (reviewing 24 ISP contracts); A.M. McDonald, R.W. Reeder, P.G. Kelley, L.F. Cranor, “A Comparative Study of Online Privacy Policies and Formats” (reviewing six companies’ privacy policies and concluding “[o]nline privacy policies are difficult to understand”), online <http://www.springer.de/comp/lncs/index.html>).

*we watch on our television sets, what we listen to on our radios, or what we send or receive by e-mail on our computers.”*²¹

24. Otherwise, individuals could rarely if ever have reasonable expectations of privacy in their personal information held by private-sector organizations subject to *PIPEDA*, regardless of the sensitivity of the information or the manner and conditions in which it was obtained. Merely by entering into such standard form contracts of adhesion – where privacy provisions are usually not specifically brought to the attention of customers before signing, and where customers usually cannot waive or amend such terms – millions of Canadians cannot be said to have knowingly or voluntarily given their ISPs prior authority to waive their constitutional rights on their behalves. Nor have they consented *en masse* to allow their ISPs to provide the police with unrestricted access to information about their Internet browsing habits.²²

25. This Court has already rejected such a “third party consent” notion as being “inconsistent with this Court’s jurisprudence,” which instead insists upon voluntary consent based on sufficiently clear information in order to make a meaningful choice.²³

26. Section 7(3)(c.1)(ii) of *PIPEDA* provides for discretionary, not mandatory, disclosures of personal information in highly exceptional circumstances. Courts have recognized that ISPs have widely varying practices in responding to police requests for disclosure of ISP subscriber information.²⁴ As this Court recently noted, individuals’ constitutional rights against state intrusion should not depend on which ISP they choose.²⁵

²¹ *R v. Gomboc*, [2010] 3 S.C.R. 211, ¶101, McLachlin C.J. and Fish J., dissenting (emphasis added); see also Scassa, above, note 15, p. 211.

²² *Gomboc*, *id.*, ¶139; *Cole*, above, note 13, ¶¶77-79. See also A. Slane and L.M. Austin, “What’s In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations” (2011), 57 *Crim. L.Q.* 486, pp. 490, 506.

²³ *Cole*, *id.*, ¶¶77-78.

²⁴ *R v. Trapp* 2011 SKCA 143, ¶56.

²⁵ *R. v. TELUS Communications Co.*, 2013 SCC 16, ¶13.

27. In any event, even if the Court were to find that the terms of service agreements with ISPs could diminish an individual's reasonable expectation of privacy, a "reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s. 8 of the *Charter*."²⁶ Accordingly, the police would still require the authority of a reasonable law, providing for prior judicial authorization, to lawfully access such information.

28. The Court of Appeal also erred in finding that "where there is informed consent the personal information protection or privacy aspects of *PIPEDA* do not further come into play."²⁷ Even with supposed consent under the terms of the service agreement, s. 5(3) of *PIPEDA* additionally requires that personal information be collected, used, or disclosed only for purposes "that a reasonable person would consider appropriate in the circumstances." Thus, "regardless of the terms of the agreement, the data subject may retain an expectation of privacy in the data that would prevent disclosure without judicial authorization. ***This would occur if the data is of a kind in which a strong and reasonable expectation of privacy would exist.***"²⁸

29. Evaluating the "appropriateness" under s. 5(3) of the *PIPEDA* of an ISP disclosing subscriber information to the police requires a case-by-case approach, not a fettering of discretion or a blanket third-party waiver in advance. Thus, even if the subscriber agreement supposedly provides for consent to disclose information, *PIPEDA* still requires an ISP to carefully weigh a customer's privacy interests against the needs of the police when seeking subscriber information.²⁹

²⁶ *Cole*, above, note 13, ¶9.

²⁷ *R. v. Spencer*, 2011 SKCA 144, ¶37.

²⁸ Scassa, above, note 15, p. 212 (emphasis added); see also A. Slane, "Privacy and Civic Duty in *R. v. Ward*: The Right to Online Anonymity and the Charter Compliant Scope of Voluntary Cooperation with Police Requests", (2013) Queen's L.J. (forthcoming), pp. 5, 13-14.

²⁹ *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, ¶¶13, 126-127.

5. The Seriousness of Child Pornography Offences Should Not Diminish The Reasonable Expectations of Privacy of Ordinary Canadians on the Internet

30. Lastly, because this case obviously has broad implications for the rights of all Canadians to be protected against state intrusion into some of the most intimate aspects of their private lives, the Court must be vigilant in ensuring that the analytic steps under ss. 8 and 24(2) of the *Charter* are kept appropriately distinct. This is essential to avoid diminishing the privacy rights of everyone merely because an accused is alleged to have engaged in serious criminal behaviour online.

31. Thus, as decided in this Court's past jurisprudence, the question of whether a person enjoys a reasonable expectation of privacy in information held by an ISP capable of identifying his online activities must be framed in "broad and neutral terms," in order to evaluate whether "in a society such as ours" this expectation is deserving of constitutional protection, irrespective of whether criminal behaviour is alleged.³⁰ The seriousness of child pornography offences can factor into the reasonableness of the search³¹ or the admissibility of the evidence,³² but should not factor into the determination of whether the accused had a reasonable expectation of privacy. Such a principled approach ensures that the constitutional privacy rights of all Canadians are not diminished as the unfortunate by-product of attempting to combat the very serious problems posed by child pornography.

³⁰ *R v. Wong*, [1990] 3 S.C.R. 36, pp. 49-50; *Patrick*, above, note 13, ¶32.

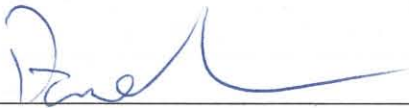
³¹ *Tessling*, above, note 8, ¶64.

³² *Cole*, above, note 13, ¶134; *R. v. Grant*, [2009] 2 S.C.R. 353, ¶84.

PART III – ORDER SOUGHT

32. The Privacy Commissioner takes no position on the disposition of this appeal. She does not seek costs and asks that no costs be awarded against her. She also asks for leave to present 10 minutes of oral argument at the hearing of the appeal.

All of which is respectfully submitted this 23rd day of August, 2013.



Mahmud Jamal
Patricia Kosseim
Daniel Caron
Sarah Speevak

Counsel for the Intervener,
Privacy Commissioner of Canada

PART IV – TABLE OF AUTHORITIES

<i>Caselaw</i>	<i>Para cited</i>
<i>C. (S.), Re</i> , 2006 ONCJ 343	19
<i>Dagg v. Canada (Minister of Finance)</i> , [1997] 2 S.C.R. 403	9
<i>Eastmond v. Canadian Pacific Railway</i> , 2004 FC 852	29
<i>Girao v. Zarek Taylor Grossman Hanrahan LLP</i> , 2011 FC 1070	9
<i>H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)</i> , [2006] 1 S.C.R. 441	9
<i>Lavigne v. Canada (Office of the Commissioner of Official Languages)</i> , [2002] 2 S.C.R. 773	9
<i>Nammo v. TransUnion of Canada Inc.</i> , 2010 FC 1284	9
<i>Pro Swing Inc. v. Elta Golf Inc.</i> , [2006] 2 S.C.R. 612	9
<i>Royal Bank of Canada v. Ren</i> , 2009 ONCA 48	9, 12
<i>R. v. A.M.</i> , [2008] 1 S.C.R. 569	19
<i>R. v. Buhay</i> , [2003] 1 S.C.R. 631	11
<i>R. v. Cole</i> , [2012] 3 S.C.R. 34	17, 24, 25, 27, 31
<i>R. v. Dyment</i> , [1988] 2 S.C.R. 417	17
<i>R. v. Evans</i> , [1996] 1 S.C.R. 8	11
<i>R. v. Gomboc</i> , 2010 SCC 55	23, 24
<i>R. v. Grant</i> , [2009] 2 S.C.R. 353	31
<i>R. v. Kang-Brown</i> , [2008] 1 S.C.R. 456	11
<i>R. v. Law</i> , [2002] 1 S.C.R. 227	11
<i>R. v. MacInnis</i> , [2007] O.J. No. 2930 (S.C.J.)	19
<i>R. v. Mahmood</i> , [2008] O.J. No. 3922 (S.C.J.)	19
<i>R. v. Morelli</i> , [2010] 1 S.C.R. 253	20

<i>R. v. Patrick</i> , [2009] 2 S.C.R. 579	17, 19, 31
<i>R. v. Plant</i> , [1993] 3 S.C.R. 281	17
<i>R. v. TELUS Communications Co.</i> , 2013 SCC 16	26
<i>R. v. Tessling</i> , [2004] 3 S.C.R. 432	11, 31
<i>R. v. Tse</i> , 2012 SCC 16	11, 12, 14
<i>R v. Trapp</i> , 2011 SKCA 143	26
<i>R. v. Vasic</i> , [2009] O.J. No. 685 (S.C.J.)	19
<i>R. v. Ward</i> , 2012 ONCA 660	11, 16
<i>R. v. Wise</i> , [1992] 1 S.C.R. 527	11
<i>R v. Wong</i> , [1990] 3 S.C.R. 36	31
<i>Wansink v. TELUS Communications Inc.</i> , 2007 FCA 21	10
<i>Doctrine</i>	
A.M. McDonald, R.W. Reeder, P.G. Kelley, and L.F. Cranor. “A Comparative Study of Online Privacy Policies and Formats”. Privacy Enhancing Technologies Symposium 2009; Internet Society, “Global Internet User Survey Summary Report” (2012), online: www.internetsociety.org/internet/global-internet-user-survey-2012	23
Andrea Slane & Lisa M. Austin, “What’s in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations” (2011) 57 Crim. L.Q. 486	24
Andrea Slane, “Privacy and Civic Duty in <i>R. v. Ward</i> : The Right to Online Anonymity and the Charter Compliant Scope of Voluntary Cooperation with Police Requests”, Queen’s L.J. (forthcoming, fall 2013)	28
Daphne Gilbert, Ian R. Kerr and Jena McGill, “The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers” (2007) 51 Crim. L.Q. 470	19
House of Commons Debates, No. 9 (22 October 1999) at 1015 (Hon. John Manley)	12

Jena McGill and Ian Kerr, “Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment” in <i>Digital Enlightenment Yearbook</i> , ed. J. Bus et al. (IOS press, 2012), at 212-216	19
Joshua J. McIntyre, “Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected As Personally Identifiable Information”, 60 <i>DePaul L. Rev.</i> (2011) at 2-7	19
Office of the Privacy Commissioner of Canada, <i>What an IP Address Can Reveal About You: A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada</i> , May 2013, available at: www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp	19
Sandra Braman and Stephanie Roberts, “Advantage ISP: Terms of Service as Media Law” in <i>New Media Society</i> 2003 5: 422	23
Stephanie Perrin, Heather H. Black, David H. Flaherty and T. Murray Rankin, “The Personal Information Protection and Electronic Documents Act: An Annotated Guide”(Toronto: Irwin Law Inc., 2001)	12
Teressa Scassa, “Information Privacy in Public Space: Location Data, Data Protection, and the Reasonable Expectation of Privacy”, (2010) 7 <i>Can. J. L. & Tech.</i> 193	19, 23, 28

PART V – TABLE OF STATUTES

<i>Personal Information Protection and Electronic Documents Act (“PIPEDA”), S.C. 2000, c. 5, s. 3, 5(3), 7(3)(c) and 7(3)(c.1)(ii).</i>	<i>Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c 5, art. 3, 5(3), 7(3)(c) et 7(3)(c.1)(ii).</i>
Purpose 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. 5. Appropriate purposes (3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. 7. Disclosure without knowledge or consent (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization; (b) for the purpose of collecting a debt owed by the individual to the organization; (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of	Objet 3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l’échange de renseignements, des règles régissant la collecte, l’utilisation et la communication de renseignements personnels d’une manière qui tient compte du droit des individus à la vie privée à l’égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d’utiliser ou de communiquer des renseignements personnels à des fins qu’une personne raisonnable estimerait acceptables dans les circonstances. 5. Fins acceptables (3) L’organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu’à des fins qu’une personne raisonnable estimerait acceptables dans les circonstances. 7. Communication à l’insu de l’intéressé et sans son consentement (3) Pour l’application de l’article 4.3 de l’annexe 1 et malgré la note afférente, l’organisation ne peut communiquer de renseignement personnel à l’insu de l’intéressé et sans son consentement que dans les cas suivants : a) la communication est faite à un avocat — dans la province de Québec, à un avocat ou à un notaire — qui représente l’organisation; b) elle est faite en vue du recouvrement d’une créance que celle-ci a contre l’intéressé; c) elle est exigée par assignation, mandat ou ordonnance d’un tribunal, d’une personne ou d’un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

information, or to comply with rules of court relating to the production of records; (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;	c.1) elle est faite à une institution gouvernementale — ou à une subdivision d’une telle institution — qui a demandé à obtenir le renseignement en mentionnant la source de l’autorité légitime étayant son droit de l’obtenir et le fait, selon le cas : (i) qu’elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales, (ii) que la communication est demandée aux fins du contrôle d’application du droit canadien, provincial ou étranger, de la tenue d’enquêtes liées à ce contrôle d’application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d’application, (iii) qu’elle est demandée pour l’application du droit canadien ou provincial;
---	---

<i>The <u>Constitution Act, 1982</u>, being Schedule B to the <u>Canada Act 1982 (UK), 1982, c 11</u>, s. 8.</i> Search or seizure 8. Everyone has the right to be secure against unreasonable search or seizure.	<i>Loi constitutionnelle de 1982 (R-U), constituant l'annexe B de la <u>Loi de 1982 sur le Canada (R-U), 1982, c 11</u>, art. 8.</i> Fouilles, perquisitions ou saisies 8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.
<i>Criminal Code, RSC 1985, c C-46, s. 487.014.</i> Power of peace officer 487.014 (1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing. Application of section 25 (2) A person who provides documents, data or information in the circumstances referred to in subsection (1) is deemed to be authorized to do so for the purposes of section 25. 2004, c. 3, s. 7.	<i>Code criminel, LRC 1985, c C-46, art. 487.014</i> Pouvoir de l'agent de la paix 487.014 (1) Il demeure entendu qu'une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix ou un fonctionnaire public chargé de l'application ou de l'exécution de la présente loi ou de toute autre loi fédérale demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune règle de droit n'interdit à celle-ci de communiquer. Application de l'article 25 (2) La personne qui fournit des documents, données ou renseignements dans les circonstances visées au paragraphe (1) est, pour l'application de l'article 25, réputée être autorisée par la loi à le faire. 2004, ch. 3, art. 7.