

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

Interveners

FACTUM OF THE INTERVENER
The Canadian Civil Liberties Association

**Anil K. Kapoor /
Lindsay L. Daviau**
KAPOOR BARRISTER
20 Adelaide Street East
Suite 210
Toronto, Ontario
M5C 2T6

Tel: 416-363-2700
Fax: 416-368-6811

Email: akk@kapoorbarristers.com

Counsel to the Intervener,
The Canadian Civil Liberties Association

Lawrence Greenspon
GREENSPON, BROWN & ASSOCIATES
331 Somerset Street West
Ottawa, Ontario
K1R 5J8

Tel: 613-288-2890
Fax: 613-288-2896

Email: email@lgreenspon.com

Ottawa Agents for the Intervener,
The Canadian Civil Liberties Association

Court File No. 34644

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 –

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

Interveners

FACTUM OF THE INTERVENER
The Canadian Civil Liberties Association

**Anil K. Kapoor /
Lindsay L. Daviau**
KAPOOR BARRISTER
20 Adelaide Street East
Suite 210
Toronto, Ontario
M5C 2T6

Tel: 416-363-2700
Fax: 416-368-6811

Email: akk@kapoorbarristers.com

***Counsel to the Intervener,
The Canadian Civil Liberties Association***

Lawrence Greenspon
GREENSPON, BROWN & ASSOCIATES
331 Somerset Street West
Ottawa, Ontario
K1R 5J8

Tel: 613-288-2890
Fax: 613-288-2896

Email: email@lgreenspon.com

***Ottawa Agents for the Intervener,
The Canadian Civil Liberties Association***

TO:

**Aaron A. Fox, Q.C. and
Darren K. Kraushaar**
MCDOUGALL GAULEY LLP
1500-1881 Scarth Street 300
Regina, Saskatchewan
S4P 4K9

Tel: (306) 565-5147
Fax: (306) 359-0785
Email: afox@mcdougallgauley.com

Counsel for the Appellant

Anthony B. Gerein
ATTORNEY GENERAL
FOR SASKATCHEWAN
3rd Floor, 1874 Scarth Street
Regina, Saskatchewan
S4P 3V7

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

Counsel for the Respondent

Jolaine Antonio
ATTORNEY GENERAL FOR ALBERTA
3rd Floor, Centrium Place
300, 332 – 6 Avenue S.W.
Calgary, Alberta
T2P 0B2

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

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

Ronald C. Reimer
Public Prosecution Services of Canada
700 EPCOR Tower 10423
101st Street
Edmonton, Alberta
T4H 0E7

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

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

Jeffrey W. Beedell
MCMILLAN LLP
300 – 50 O'Connor Street
Ottawa, Ontario
K1P 6L2

Tel: (613) 232-7171
Fax: (613) 231-3191
Email: jbeedell@mcmillan.ca

Agent for the Appellant

Henry S. Brown, Q.C.
GOWLING LAFLEUR HENDERSON LLP
2600 – 160 Elgin Street
Ottawa, Ontario
K1P 1C3

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

Agent for the Respondent

Brian A. Crane, Q.C.
GOWLING LAFLEUR HENDERSON LLP
2600 – 160 Elgin Street
Ottawa, Ontario
K1P 1C3

Tel: (613) 233-1781
Fax: (613) 563-9863
Email: brian.crane@gowlings.com

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

Francois Lacasse
Directeur des poursuites penales du
Canada
284 rue Wellington
Ottawa, Ontario
K1A 0H8

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

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

Susan Magotiaux and Alison Dellandrea
 ATTORNEY GENERAL OF ONTARIO
 Crown Law Office – Criminal
 720 Bay Street, 10th Floor
 Toronto, Ontario
 M5G 2K1

Tel: (416) 326-5238
 Fax: (416) 326-4656
 Email: susan.magotiaux@ontario.ca

Counsel for the Intervener
Attorney General of Ontario

Jill R. Presser and Jonathan Dawe
 SCHRECK PRESSER LLP
 5th Floor, 6 Adelaide Street East
 Toronto, Ontario
 M5C 1H6

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

Counsel for the Intervener
Criminal Lawyers' Association

Mahmud Jamal and Patricia Kosseim
 OSLER, HOSKIN & HARCOURT LLP
 1 First Canadian Place
 Toronto, Ontario
 M5X 1B8

Tel: (416) 862-6764
 Fax: (416) 862-6666
 Email: mjamal@osler.com

Counsel for the Intervener
Privacy Commissioner of Canada

Robert E. Houston, Q.C.
 BURKE-ROBERTSON
 441 MacLaren Street
 Suite 200
 Ottawa, Ontario
 K2P 2H3

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

Agent for the Intervener
Attorney General of Ontario

Supreme Advocacy LLP
 397 Gladstone Avenue
 Suite 1
 Ottawa, Ontario
 K2P 0Y9

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

Agent for the Intervener
Criminal Lawyers' Association

Daniel Caron
 OFFICE OF THE PRIVACY
 COMMISSIONER OF CANADA
 112 Kent Street, 3rd Floor
 K1A 1H3

Tel: (613) 947-4634
 Fax: (613) 647-4193
 Email: daniel.caron@priv.gc.ca

Agent for the Intervener
Privacy Commissioner of Canada

TABLE OF CONTENTS

PART I – OVERVIEW	1
PART II – ARGUMENT	3
A. Need for a Broad and Neutral Formulation of the Issue Raised.....	3
B. A Reasonable Expectation of Privacy is Implicated.....	4
C. PIPEDA Should be Interpreted to Protect (Not Defeat) Privacy.....	7
D. The Effect of Service Agreements with Internet Service Providers.....	7
E. The Proper Construction of Section 487.014(1) of the Criminal Code.....	10
PART III – ORDER SOUGHT.....	10
PART IV – TABLE OF AUTHORITIES.....	11
PART V – TABLE OF STATUTES.....	13

Court File No. 34644

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 –

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

Interveners

FACTUM OF THE INTERVENER
The Canadian Civil Liberties Association

PART I – OVERVIEW

1. Privacy is both an individual right, essential for personal autonomy and dignity, and a societal good, a necessary underpinning for a functional democracy where individuals, groups and institutions have the freedom to debate, discuss, investigate, associate and organize free from the fear of state surveillance. At issue on this appeal is the reasonable expectation of privacy enjoyed by Canadians when using the Internet. Specifically, whether or not section 8 of the *Canadian Charter of Rights and Freedom*¹ (“*Charter*”) requires that police and other government actors obtain a warrant to pierce the anonymity of an Internet Protocol address (“IP address”) and gain access to the identity of an Internet user. The implications of this appeal are profound. Revealing such information is the key to connecting an individual to their online activities. Although the issue arises in the context of a criminal prosecution involving Mr. Spencer, who was alleged to have used his Internet connection to download

¹ Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

and share child pornography, the case has much broader privacy implications. The anonymity provided by an IP address is what shields the privacy of *all* Canadians when they use the Internet.

2. By way of overview, the Canadian Civil Liberties Association (“CCLA”) makes the following submissions on this appeal:

- That this Court’s section 8 *Charter* jurisprudence requires a broad and neutral formulation of the privacy issue raised by this case. Therefore, the question to be decided is *not* simply whether someone who downloads and shares child pornography, contrary to the terms of the standard form contract with their Internet Service Provider, enjoys a reasonable expectation of privacy in information that would connect them to their online activities. Casting the question in such narrow terms involves a prohibited form of *ex post facto* reasoning. Rather, broadly framed, the question is whether or not Canadians would reasonably expect that police be required to obtain a warrant in order to pierce the anonymity provided by their IP addresses and thereby connect them to their online activities? (See ¶3 to ¶4.)
- Internet browsing and surfing activities tend to reveal intimate details about a person’s lifestyle and personal choices such that the consequences of lifting the anonymity provided by an IP address are profound and widespread. As a result, such information is subject to a reasonable expectation of privacy and the protection of section 8 of the *Charter*. Because piercing the anonymity supplied by an IP address is the key to connecting an individual to their online activities, the CCLA submits that section 8 of the *Charter* is engaged by such an intrusion. (See ¶5 to ¶12.)
- That the *Personal Information Protection and Electronic Documents Act*² (“PIPEDA”) PIPEDA, the purpose of which is to *protect* the privacy of Canadians, should not be construed so as to license warrantless access to the subscriber information behind IP addresses. To the extent that lower courts have construed PIPEDA in this way, it is submitted that such an interpretation is in error. (See ¶13.)
- That the terms contained in standard form contracts between Internet Service Providers and their subscribers should not be decisive of the scope of an individual’s constitutionally protected privacy interests. The scope of the protection afforded by section 8 of the *Charter* is a normative question that cannot be directed or determined either by legislation or by the fine print of rarely read or understood contractual terms. Further, allowing such contractual terms to defeat a privacy claim involves the very sort of *ex post facto* reasoning that this Court’s section 8 jurisprudence has consistently eschewed. (See ¶14 to ¶19.)
- Finally, that section 487.014(1) of the *Criminal Code* should be construed as only authorizing police to access data, documents or information that is not subject to a reasonable expectation of privacy and therefore does not engage section 8 of the *Charter*. Absent exigent circumstances,

² SC 2000, c 5 [PIPEDA].

information that is subject to a reasonable expectation of privacy should only be accessed with a warrant. (See ¶20.)

The *CCLA* also adopts the submissions made by the Privacy Commissioner of Canada and the Criminal Lawyers' Association of Ontario in their respective facts. The *CCLA* takes no position with respect to the other legal issues raised by the Appellant.

PART II – ARGUMENT

A. Need for a Broad and Neutral Formulation of the Issue Raised

3. It is submitted that most lower courts that have dealt with the issue raised by this appeal, including the court below in this case, have taken too narrow an approach. They have unduly focused their analysis on the particular activities of the accused, who are invariably individuals who used the Internet to view, download and/or trade in child pornography.³ However, this Court has repeatedly cautioned against the use of *ex post facto* reasoning in evaluating constitutional claims under section 8 of the *Charter*,⁴ explaining that the purpose of the guarantee “is to prevent unreasonable intrusions on privacy, not to sort them out from reasonable intrusions on an *ex post facto* analysis”.⁵ According to this Court, this approach is “inherent in the notion of being secure against unreasonable searches and seizures”.⁶ As a result, this Court has directed that decisions as to whether or not section 8 is engaged must be made from an *ex ante* perspective, without regard to the fact that evidence of illegal activity was discovered. In evaluating claims under section 8 of the *Charter*, “the question must be framed in broad and neutral terms”.⁷ This approach requires a reviewing court to ask what law-abiding Canadians would reasonably expect in the circumstances.⁸

4. It is submitted that when framed in broad and neutral terms, the question presented by this appeal is whether, in a society such as ours, persons have a reasonable expectation of privacy in their online activities including their association with an IP address.

³ See e.g. *R v Ward*, 2012 ONCA 660, 112 OR (3d) 321 [*Ward*].

⁴ See *Hunter v Southam Inc.*, [1984] 2 SCR 145 at 160, 14 CCC (3d) 97; *R v Wong*, [1990] 3 SCR 36 at 49-50, 60 CCC (3d) 460 [*Wong*]; *R v Greffe*, [1990] 1 SCR 755 at 775, 790, 55 CCC (3d) 161; *R v Dyment*, [1988] 2 SCR 417 at para 23, 45 CCC (3d) 244 [*Dyment*]; *R v Kokesh*, [1990] 3 SCR 3 at para 46, 61 CCC (3d) 207; *R v Feeney*, [1997] 2 SCR 13 at paras 45, 49, 52 115 CCC (3d) 129 [*Feeney*]; *R v Buhay*, 2003 SCC 30 at para 19, [2003] 1 SCR 631 [*Buhay*]; *R v A.M.*, 2008 SCC 19 at paras 5, 70, [2008] 1 SCR 569.

⁵ *Feeney*, *supra* note 4 at para 45.

⁶ *Dyment*, *supra* note 4 at 430.

⁷ *Wong*, *supra* note 4 at 50. See also *Buhay*, *supra* note 4 at para 19.

⁸ *Ibid*

B. A Reasonable Expectation of Privacy is Implicated

5. It is submitted that Canadians enjoy a reasonable expectation of privacy in their internet browsing and surfing activities that is deserving of section 8 *Charter* protection. An individual's activities on the Internet can reveal highly personal and intimate information⁹ about that person, and provide considerable insight into the user's interests, habits, predilections and, by implication, their very thoughts.¹⁰ Because piercing the anonymity supplied by an IP address is the key to unlocking a vast repository of highly personal information regarding an individual's online activities, it is submitted that section 8 of the *Charter* is engaged by such an intrusion.

6. With respect, it is submitted that Ottenbreit J.'s conclusion (in the court below) that there was no privacy expectation in the information at issue in this case, which he characterized as "simply name, address and telephone number"¹¹ – a position also advanced by the Respondent before this Court¹² – fails to place the informational privacy interest implicated in these circumstances in its proper context. This Court has emphasized that when it comes to determining whether a reasonable expectation of privacy is engaged, "[t]he assessment *always* requires close attention to context."¹³

7. To be sure, as the Respondent argues, in the abstract, an individual's name, address and telephone number are not inherently private information. However, depending on the context, they can be. Where such information is the key to unlocking a wealth of personal information about that individual, maintaining anonymity can be integral to ensuring privacy.¹⁴ Professor Alan Westin, a

⁹ See *R v Plant*, [1993] 3 SCR 281 at 293, 84 CCC (3d) 204, which recognizes that section 8 is engaged when information is accessed that, "tends to reveal intimate details of the lifestyle and personal choices of the individual."

¹⁰ The analysis in *R v Morelli*, 2010 SCC 8 at para 3, [2010] 1 SCR 253 is arguably supportive, wherein Fish J, for the majority, emphasized that one of the reasons computer searches are so invasive is because they permit: "[t]he police [to] scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident." See also *BMG Canada Inc. v Doe*, 2005 FCA 193 at para 4, 252 DLR (4th) which acknowledged the importance of maintaining privacy in relation to Canadians' online activities.

¹¹ See *R v Spencer*, 2011 SKCA 144, 283 CCC (3d) 384 at paras 109-110, Ottenbreit J., concurring.

¹² See Factum of the Respondent, at para. 44.

¹³ *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579 at para 26 [italics added]. See also *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 at para 23 [*Gomboc*]: "I reiterate before undertaking that analysis that context is crucial and that reasonable expectation of privacy is assessed in the totality of the circumstances."

¹⁴ See e.g. *R v Eddy* (1994) 119 Nfld & PEIR 91 at para 175 (available on CanLII) (NLSC (TD)), making this point in the context of banking records, explaining that: "The linkage of a name to [account] information creates at once the intimate relationship between that information and the particular individual, which is the essence of the privacy interest. I do not accept the Crown's suggestion that the mere obtaining of the name of the owner of an account about which information is already available is not deserving of protection under s. 8."

leading American privacy expert, recognized that anonymity can sometimes be essential for privacy. He explained:

The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behaviour and role that would operate if he were known to those observing him. In this state the individual is able to merge into the “situational landscape.” Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.¹⁵

8. The Internet has quickly become an established part of modern life. Moreover, the Internet is an integral and for some essential part of daily life, enabling and facilitating purposes that are not only lawful, but enhance a democratic free society and are an integral part of one’s liberty and free expression. The ability to link Internet users to the websites they have visited would reveal a host of intimate details about the user’s lifestyle and personal choices. The Federal Court of Appeal has acknowledged how integral the Internet has become in the lives of Canadians and the depth of personal information that is available:

Citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed. This intrusion not only puts individuals at great personal risk but also subjects their views and beliefs to untenable scrutiny.¹⁶

9. The collective understanding that has led members of the public to embrace the Internet for such varied purposes was recognized by Wilkins J., who noted that, “[g]enerally speaking, it is understood that a person’s internet protocol address will not be disclosed.”¹⁷ Once it is, as Pringle J. explained in *Cuttell*, it serves to reveal, “intimate details of a subscriber’s lifestyle and choices. Once the police accessed Mr. Cuttell’s name and address, they were able to link his identity to a wealth of intensely personal information.”¹⁸ It is therefore not at all surprising that the Privacy Commissioner of Canada has

¹⁵ Alan F Westin, *Privacy and Freedom* (New York: Athenum, 1967), at 32. See also 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 LQ 486 at 501-503.

¹⁶ *BMG Canada Inc. v Doe*, 2005 FCA 193 at para 4, 252 DLR (4th) 342.

¹⁷ *Irwin Toy Ltd v Doe*, (2000) 12 CPC (5th) 103 at para 10, 99 ACWS (3d) 399. (The case involved a plaintiff seeking to compel an Internet Service Provider to disclose the identity of the user behind a particular IP address, in order to pursue a defamation action.)

¹⁸ *R v Cuttell*, 2009 ONCJ 471, 247 CCC (3d) 424 at para 21, aff’d on other grounds 2012 ONCA 661.

recommended that basic subscriber information, like the name and address of an Internet user connected to a particular IP address, should only be accessible with a warrant.¹⁹

10. Those who use the Internet have justifiably come to expect anonymity, as it is essential to shielding their privacy. Should this Court conclude that Canadians do not enjoy a reasonable expectation of privacy that protects against unwarranted disclosure of an Internet user's identity, the potential effect on how the Internet is used, especially by those on the social and political margins, could be profound. As Professor Renke has warned,

The consequences of this loss of privacy cannot be properly predicted now. If individuals understand that they are constantly under surveillance, a "chilling" effect may occur -- particularly if individuals perceive data mining to be just one of multiple State surveillance techniques. Individuals may constrain their freedoms of belief, expression or association, for fear of generating suspicious patterns.²⁰

11. Professor Renke's fears are not unfounded: data mining is routinely used to scoup up and collect vast amounts of information. The collection of what has been termed 'metadata' is vast and when assessed permits the state a detailed view into the everyday private lives of Canadians.²¹ Clearly, the technology to engage in such practices exists.. What remains is the constitutional question; whether or not the state should be permitted to link an Internet user to their online activities without the need to first justify such an intrusion to a judge.

¹⁹See Office of the Privacy Commissioner of Canada, *Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada*, October 2007, at 6, online: < http://www.priv.gc.ca/information/pub/lar_071108_e.pdf>.

²⁰ Wayne N Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy (2006), 43 Alta L Rev 779 at para 50. See also Arthur J Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007), 40 UBC L Rev 41 at 52

²¹Metadata is 'transactional' information generated by our smartphones, personal computers and tablets. This information can reveal the time and duration of your communications, the particular devices used, email addresses or numbers contacted, and at what locations. Since virtually every device has a unique identifying number, all communications and Internet activities may be linked together and traced, with relative ease. This information can reveal a great deal about an individual including where they live, sleep, travel, on-line purchases, networks of friends, family and associates, as well as details as intimate as when you go to sleep and when you wake up.

Existing government surveillance programs (such as those run for example by the U.S. National Security Agency (NSA)) systematically gather and analyze vast quantities of metadata for different purposes. Armed with this data, the state has the power to instantaneously create a detailed digital profile of the life of anyone swept up in such a massive data seizure. Once this data is compiled and examined, detailed pictures of individuals begin to emerge. The data can reveal your political or religious affiliations, as well as your personal and intimate relationships.

See Ann Covoukian, Office of the Information and Privacy Commissioner, Ontario, Canada, *A Primer on Metadata: Separating Fact from Fiction*, July 2013, online: <http://www.ipc.on.ca/images/Resources/metadata.pdf>.

12. The CCLA submits that Internet users do have a reasonable expectation of privacy in information that would disclose their connection to an IP address and thereby serve to reveal their online activities.

C. PIPEDA Should be Interpreted to Protect (Not Defeat) Privacy

13. It is submitted that *PIPEDA*, the purpose of which is to *protect* the privacy of Canadians,²² should not be construed so as to license warrantless access to the subscriber information behind IP addresses. To the extent that lower courts have construed subsection 7(3)(c.1) of *PIPEDA* in this way, as did Caldwell JA in the court below, it is submitted that this interpretation is in error. Properly construed, in light of its plain wording, the larger purposes of *PIPEDA*, and *Charter* values, that provision simply creates an exception to the general obligation on “organizations” to keep “personal information” they acquire confidential.²³ Subsection 7(3)(c.1) enables an organization to comply with law enforcement requests, *provided* the request is premised on “lawful authority”. In short, this provision does *not* create any *new* police search and seizure powers.²⁴ Rather, it merely facilitates the execution of *existing* powers. In the criminal investigative realm, the established lawful authority by which police may intrude upon a reasonable expectation of privacy, absent exigent circumstances, is a warrant.

D. The Effect of Service Agreements with Internet Service Providers

14. This Court’s decision in *R. v. Gomboc*²⁵ provides essential guidance on the constitutional significance of the terms found in contractual agreements governing the release of information about customers by a business. The issue in *Gomboc* was whether the installation of a digital recording ammeter to measure the flow of electricity entering a home encroached upon a reasonable expectation of privacy, so as to engage s. 8 of the *Charter*. The terms of the contractual arrangement between the utility and the customer, which were dictated by a provincial regulation, entitled the utility to divulge, “customer information” — that is, information “not available to the public” that “is uniquely associated with a customer” — “to a peace officer for the purpose of investigating an offence” so long as “the disclosure is not contrary to the express request of the customer”.²⁶ Writing for the plurality, Deschamps J. addressed the role of such agreements in assessing the existence of a reasonable expectation of privacy,

²² See *PIPEDA*, *supra* note 2 at s 3.

²³ *Ibid* s 5(1).

²⁴ See *House of Commons Debates*, 36th Parl, 2nd Sess, No 9 (22 October 1999) at 1015 (Hon John Manley]. See also *Royal Bank of Canada v Ren*, 2009 ONCA 48 at para 22, 93 OR (3d) 403 (coming to the same conclusion regarding the exceptions found in subsections 7(3)(d)(i) and 7(3)(h.2) of *PIPEDA*, which relate to the banking sector).

²⁵ *Gomboc*, *supra* note 13.

²⁶ *Ibid* at paras 83-84, Abella J concurring.

explaining:

[33] That [the utility] was at liberty to disclose the information weighs heavily against giving the asserted expectation of privacy constitutional recognition. However, in view of the multitudinous forms of information that are generated in customer relationships and given that consumer relationships are often governed by contracts of adhesion (while noting that in this case Mr. Gomboc was at liberty to prevent the disclosure but did not elect to do so), there is every reason for proceeding with caution when deciding what independent constitutional effect disclosure clauses similar to those in the Code of Conduct Regulation may have on determining a reasonable expectation of privacy.

[34] Even if the regulation had been silent on disclosure of energy consumption, the quality and nature of the information disclosed to the police would nonetheless have informed the totality of the circumstances surrounding the expectation of privacy. Determining the expectation of privacy requires examination of whether disclosure involved biographical core data, revealing intimate and private information for which individuals rightly expect constitutional privacy protection. This is consistent with Binnie J.'s comment in Tessling that the expectation of privacy is a "normative rather than a descriptive standard" (para 42). Thus, the fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative. Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved, the reasons why it was collected, and the circumstances in which it was intended to be used.²⁷

15. Consequently, the fact that a statute or contract permits disclosure to police is not determinative as to whether or not section 8 of the *Charter* is engaged. As Chief Justice McLachlin and Justice Fish stated in *Gomboc*, "legislation is only one factor that is to be considered when determining whether an expectation of privacy is objectively reasonable and it may be insufficient to negate an expectation of privacy that is otherwise particularly compelling."²⁸ The same is true of commercial contracts of adhesion, like the contract in this case, which cannot be read as single-handedly subverting otherwise valid privacy expectations.

16. The terms of the contract between the Appellant and Shaw figured prominently in Caldwell JA's analysis in the court below.²⁹ However, *Gomboc* makes clear that such contractual provisions should be put in their proper context when assessing the "totality of circumstances". It must be recognized that these sorts of terms have become pervasive *because of PIPEDA*. Section s. 5(1) of the *PIPEDA* requires every organization to "comply with the obligations set out in Schedule 1" of the Act, and that schedule mandates that organizations must disseminate to their clients and customers information about their privacy policies and procedures,³⁰ including information about the circumstances in which personal

²⁷ *Ibid* at paras 33-34, Deschamps J concurring (joined by Charron, Rothstein and Cromwell JJ) (underlining added).

²⁸ *Ibid* at para 115, McLachlin CJ and Fish J, dissenting.

²⁹ *R v Spencer*, 2011 SKCA 144, 283 CCC (3d) 384 [*Spencer*] at paras. 28-42, Caldwell JA, concurring.

³⁰ *PIPEDA*, Schedule 1, 4.1.4(d).

information may be disclosed.³¹ It is therefore not at all surprising that many of the contractual terms between Internet users and Internet Service Providers serve to roughly track the various exceptions, to the duty owed to keep personal information confidential, that have been carved out by s. 7(3) of *PIPEDA*. Consequently, the terms found in these sorts of agreements should not be construed so as to defeat an Internet user's reasonable expectations of privacy in information that would reveal their connection to an IP address and serve to expose their surfing and browsing activities while online to state scrutiny. It would be most ironic if contractual terms that have effectively been mandated by *PIPEDA*, legislation that was intended to protect privacy, were to ultimately serve to defeat it.

17. *Gomboc* specifically recognized the danger of allowing the fine print found in contracts of adhesion to define Canadians' reasonable privacy expectations. In reality, few users take the time to read or have the legal training to fully understand such agreements. Ultimately, as this Court noted in *Gomboc*, the scope of Canadians' reasonable privacy expectations is a normative constitutional question that cannot be prescribed by statute or defined by contract.³² As a result, contractual terms that mimic the exceptions found in s. 7(3) of *PIPEDA* should play no role in defining the scope of Canadians' privacy expectations when it comes to their use of the Internet.

18. Finally, it is submitted that allowing contractual terms, like those found in Shaw's standard form subscriber agreement, to defeat a constitutional privacy claim involves a form of *ex post facto* reasoning. These agreements only assume significance if one begins the analysis by looking at the results of a particular search. Invariably, contractual agreements relieve Internet Service Providers of any duty of confidentiality where a subscriber uses the service for an illegal purpose. (The same is arguably true of many agreements that govern commercial relationships.) But using such contractual terms in conjunction with the results of a search to conclude that there is no privacy protection involves the very sort of *ex post facto* analysis that the established section 8 *Charter* jurisprudence has long eschewed. Of course, all of this relates back to the need to formulate the issue raised in broad and neutral terms, which, as explained above, the *CCLA* submits is the appropriate approach when framing the important question raised by this appeal.

³¹ *PIPEDA*, Schedule 1, 4.8.

³² *Gomboc*, *supra* note 13 at paras 34, 115. See also *Patrick*, *supra* note 13 at para 14; See *R v Tessling*, 2004 SCC 67 at para 19, [2004] 3 SCR 432 at para. 42 [*Tessling*].

19. For all of these reasons, it is submitted that the important constitutional issue raised by this appeal should not be determined based on the language that happens to be found in the standard form contract that Shaw's customers are required to sign.


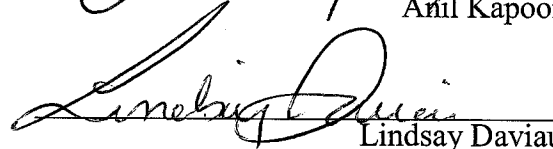
E. The Proper Construction of Section 487.014(1) of the Criminal Code

20. It is submitted that, contrary to the view expressed by Cameron JA in the court below,³³ section 487.014(1) of the *Criminal Code* does not authorize the police to obtain any and all information without a warrant. Information that is subject to a reasonable expectation of privacy should only be accessed by state officials in compliance with procedures and standards that meet minimum section 8 *Charter* standards. Properly construed, section 487.014(1) is only relevant where the police collect "data, documents or information" that is not subject to a reasonable expectation of privacy and therefore does not involve a "search" or "seizure" from a section 8 *Charter* standpoint.³⁴

PART III – ORDER SOUGHT

21. The *CCLA* takes no position on the disposition of this appeal. Nor does the *CCLA* seek costs. It also asks that no costs be awarded against it. Finally, the *CCLA* seeks leave to present 15 minutes of oral argument at the hearing of this appeal.

All of which is respectfully submitted this 26th day of September, 2013.


Anil Kapoor

Lindsay Daviau

Counsel for the Intervener,
Canadian Civil Liberties Association

³³ This was consistent with the Court's analysis in the companion decision that it released concurrently in *R v Trapp*, 2011 SKCA 143, [2012] WWR 648.

³⁴ See *Ward*, *supra* note 3 at paras 49-50, which endorses this interpretation of section 487.014(1).

PART IV – TABLE OF AUTHORITIES**Paragraph(s)****Cases:**

<i>BMG Canada Inc. v. Doe</i> , 2005 FCA 193	5, 8
<i>Hunter v Southam Inc.</i> , [1984] 2 S.C.R. 145 at 160, 14 CCC (3d) 97	3
<i>Irwin Toy Ltd. v. Doe</i> , [2000] O.J. No. 3318 (S.C.J.)	9
<i>R v A.M.</i> , [2008] 1 S.C.R. 569, 2008 S.C.C. 19	3
<i>R. v. Buhay</i> , [2003] 1 S.C.R. 631, 2003 S.C.C. 30	3
<i>R. v. Cuttell</i> (2009), 247 C.C.C. (3d) 424 (Ont. C.J.)	9
<i>R v Dymont</i> , [1988] 2 S.C.R. 417 at 430, 45 C.C.C. (3d) 244	3
<i>R v Eddy</i> (1994), 119 Nfld & PEIR 91 (available on CanLII) (NLSC (TD))	7
<i>R v Feeney</i> , [1997] 2 S.C.R. 13, 52 115 C.C.C. (3d) 129	3
<i>R. v. Gomboc</i> , 2010 S.C.C. 55, [2010] 3 S.C.R. 211	6, 14, 15, 17
<i>R v Greffe</i> , [1990] 1 S.C.R. 755 at 775, 790, 55 C.C.C. (3d) 161	3
<i>R v Kokesch</i> , [1990] 3 S.C.R. 3 at 29, 61 C.C.C. (3d) 207	3
<i>R. v. Morelli</i> , [2010] 1 S.C.R. 253, 2010 S.C.C. 8	5
<i>R. v. Patrick</i> , [2009] 1 S.C.R. 579, 2009 S.C.C. 17	6
<i>R. v. Plant</i> , [1993] 3 S.C.R. 281	5
<i>R. v. Tessling</i> , [2004] 3 S.C.R. 432, 2004 S.C.C. 67	17
<i>R. v. Trapp</i> , 2011 SKCA 143	20
<i>R. v. Ward</i> , 2012 ONCA 660	3, 20
<i>R. v. Wong</i> , [1990] 3 S.C.R. 36	3
<i>Royal Bank of Canada v. Ren</i> , 2009 ONCA 48	13

Books and Papers:

- Office of the Privacy Commissioner of Canada, *Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada*, October 2007, online: http://www.priv.gc.ca/information/pub/lar_071108_e.pdf 9
- Wayne N Renke, “Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy (2006), 43 Alta L Rev 779 at 797. 10
- Arthur J. Cockfield, “Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies” (2007), 40 UBC L Rev 41 at 52 10
- Ann Covoukian, Office of the Information and Privacy Commissioner, Ontario, Canada, *A Primer on Metadata: Separating Fact from Fiction*, July 2013, online: <http://www.ipc.on.ca/images/Resources/metadata.pdf> 11
- House of Commons Debates*, 36th Parl, 2nd Sess, No 9 (22 October 1999) at 1015 (Hon John Manley] 13
- Alan F Westin, *Privacy and Freedom* (New York: Athenum, 1967) 7
- Slane, A. 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 C.L.Q. 7

PART V – TABLE OF STATUTES

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11:

8. Everyone has the right to be secure against unreasonable search or seizure.

* * *

24. (1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5, as amended:

2. (1) The definitions in this subsection apply in this Part.

* * *

"commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

* * *

"organization" includes an association, a partnership, a person and a trade union.

* * *

"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

* * *

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.

* * *

Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

Meaning of "should"

(2) The word "should", when used in Schedule 1, indicates a recommendation and does not impose an obligation.

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.

* * *

Collection without knowledge or consent

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(c) the collection is solely for journalistic, artistic or literary purposes;

(d) the information is publicly available and is specified by the regulations; or

(e) the collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(c.1)(i) or (d)(ii), or

(ii) that is required by law.

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;

(c.1) it is publicly available and is specified by the regulations; or

(d) it was collected under paragraph (1)(a), (b) or (e).

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 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.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section;

*(c.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) Act* as required by that section;

* [Note: Paragraph 7(3)(c.2), as enacted by paragraph 97(1)(a) of chapter 17 of the Statutes of Canada, 2000, will be repealed at a later date.]

(d) made on the initiative of the organization to an investigative body, a government institution or a

part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(h) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(h.1) of information that is publicly available and is specified by the regulations;

(h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(i) required by law.

Use without consent

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Disclosure without consent

(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(a) to (h.2).

* * *

SCHEDULE 1

(Section 5)

PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96

* * *

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

- (a) implementing procedures to protect personal information;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) training staff and communicating to staff information about the organization's policies and practices; and
- (d) developing information to explain the organization's policies and procedures.

* * *

4.8 Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

- (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards,

or codes; and

(e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

* * *

Criminal Code, SC 1985, c C-46, as amended:

487.11 A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, may, in the course of his or her duties, exercise any of the powers described in subsection 487(1) or 492.1(1) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant.

Controlled Drugs and Substances Act, SC 1996, c 19:

11(7) A peace officer may exercise any of the powers described in subsection (1), (5) or (6) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain one.

MATTHEW DAVID SPENCER and HER MAJESTY THE QUEEN and CANADIAN CIVIL LIBERTIES ASSOCIATION
APPELLANT RESPONDENT INTERVENER

Court File No. 34644

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

FACTUM OF THE INTERVENER
Canadian Civil Liberties Association

**Anil K. Kapoor /
Lindsay L. Daviau**
Kapoor Barristers
Suite 210
20 Adelaide Street East
Toronto, Ontario
M5C 2T6

(416) 363-2700

Counsel to the INTERVENER
Canadian Civil Liberties Association