

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

BETWEEN:

MATTHEW DAVID SPENCER

APPELLANT
(APPELLANT/RESPONDENT)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(RESPONDENT/APPELLANT)

APPELLANT'S FACTUM
(Pursuant to Rule 42 of the Rules of the Supreme Court of Canada)

Aaron A. Fox, Q.C. and
Darren K. Kraushaar
Counsel for Matthew David Spencer

McDougall Gauley LLP
1500-1881 Scarth Street
Regina, Saskatchewan
S4P 4K9
Tel: (306) 757-1641
Fax: (306) 359-0785
E-mail: afox@mcdougallgauley.com

Anthony B. Gerein
Counsel for the Respondent

Office of the Attorney General
for the Province of Saskatchewan
Saskatchewan Justice - Public Prosecutions
3rd Floor, 1874 Scarth Street
Regina, Saskatchewan S4P 3V7
Tel: (306) 787-5490
Fax: (306) 787-8878
E-mail: tony.gerein@gov.sk.ca

Jeffrey W. Beedell
Ottawa Agents for Counsel
for the Appellant

McMillan LLP
300 - 50 O'Connor Street
Ottawa, Ontario
K1P 6L2
Tel: (613) 232-7171
Fax: (613) 231-3191
E-mail: jbeedell@mcmillan.ca

Henry S. Brown, Q.C.
Ottawa Agents for the Respondent

Gowling Lafleur Henderson LLP
Barristers and Solicitors
2600 - 160 Elgin Street
Ottawa, Ontario K1P 1C3
Tel: (613) 232-1781
Fax: (613) 563-9869
E-mail: henry.brown@gowlings.com

TABLE OF CONTENTS

FACTUM OF THE APPELLANT

	Page
PART I	STATEMENT OF FACTS
A. Overview	1
B. Background Facts	2
C. Trial Judgment – <i>Voir Dire</i>	4
i) Section 8 Application	4
D. Trial Judgment	4
i) <i>Mens Rea</i> Requirement of Section 163.1(3) of the <i>Criminal Code</i> – Making Available Child Pornography	4
E. The Court of Appeal Judgment	7
i) Search of Information Attached to IP Address - Section 8 Application	7
ii) Wilful Blindness	9
PART II	QUESTIONS IN ISSUE
	10
PART III	STATEMENT OF ARGUMENT
Issue One: Was the Court of Appeal in error in determining that there was no reasonable expectation of privacy in the information attached to an internet protocol address?	10
A. The Nature of the Information Obtained	10
B. Section 8 Protected Privacy Interests	13
i) Application of the Analysis to the Circumstances	17
a) The Subject Matter of the Search	17
b) The Appellant’s Interest in the Subject Matter	17
c) The Place Where the Alleged Search Occurred	18
d) Was the Information in Public View	18
e) Was the Information Already in the Hands of Third Parties and, if so, was it Subject to an Obligation of Confidentiality	19

f)	Was the Police Technique Intrusive in Relation to the Privacy Interest	23
g)	Was the Evidence Gathering Technique Itself Objectively Unreasonable	23
h)	Does the Information Reveal Intimate Details of the Appellant's Lifestyle or Biography	25
ii)	Totality of the Circumstances	25
iii)	Was the Search Reasonable	27
	Issue Two: If the Appellant's rights under section 8 of the <i>Charter</i> were breached, should the evidence gathered upon the execution of the search warrant be excluded pursuant to section 24(2) of the <i>Charter</i> ?	28
A.	The Seriousness of the <i>Charter</i> Infringing State Conduct	28
B.	The Impact of the <i>Charter</i> Protected Interests of the Appellant	28
C.	Society's Interest in Adjudication on the Merits	29
	Issue Three: Did the Court of Appeal err in overturning the decision of the learned trial judge that the Appellant did not have the necessary <i>mens rea</i> to commit the offence of making available child pornography contrary to section 163.1(3) of the <i>Criminal Code</i> on the basis that he failed to consider the question of willful blindness on the part of the Appellant?	30
A.	The Decision of the Court of Appeal	30
B.	Positive Step or Action	31
C.	Wilful Blindness	33
i)	The Law Regarding the Doctrine of Wilful Blindness	34
ii)	Application to the Case at Bar	37
PART IV	SUBMISSIONS AS TO COSTS	39
PART V	ORDER REQUESTED	40
PART VI	TABLE OF AUTHORITIES	41
PART VII	STATUTORY PROVISIONS	42

FACTUM OF THE APPELLANT

PART I - STATEMENT OF THE FACTS

A. Overview

1. The Appellant, Matthew David Spencer, was charged as follows:
 - 1) Between the 31st day of August, A.D. 2007, and the 20th day of September A.D. 2007, at or near Saskatoon, in the Province of Saskatchewan, did have in his possession, child pornography to wit: Images of children under the age of 18, engaged in explicit sexual activity, contrary to Section 163.1(4) of the *Criminal Code*;
 - 2) Between the 31st day of August, A.D. 2007, and the 20th day of September, A.D. 2007, at or near Saskatoon, in the Province of Saskatchewan, make available child pornography where he did make images of children under the age of 18, engaged in explicit sexual activity available to other persons through the Internet, contrary to Section 163.1(2) of the *Criminal Code*.
2. The Appellant made application pursuant to section 24(2) of the *Canadian Charter of Rights and Freedoms*, for exclusion of the material found on his personal computer that was seized in a search of his residence. He argued that his rights under section 8 of the *Charter* had been breached. The learned trial judge rejected the argument. The Appellant's appeal to the Saskatchewan Court of Appeal was dismissed. The Court of Appeal concluded that there was no reasonable expectation of privacy in the information attached to the internet protocol address ("IP address") that had been obtained by the investigating police officer directly from the internet provider without a warrant and in the alternative, the search was not unreasonable.
3. The learned trial judge found the Appellant guilty of possession of child pornography but dismissed the charge of making child pornography available to others on the basis that the Appellant did not have the necessary *mens rea* to commit the said offence. The Court of Appeal allowed the Crown's appeal holding that it did not disagree with the trial judge's finding of fact but found that the trial judge erred in law by failing to consider whether the Appellant was guilty because of wilful blindness.

4. This appeal deals with two issues:

- 1) Is there a reasonable expectation of privacy in the information attached to an IP address; and
- 2) In the circumstances of this case, based on the findings of fact made by the trial judge, was there an issue of wilful blindness sufficient to satisfy the *mens rea* requirement of section 163.1(3) of the *Criminal Code*.

B. Background Facts

5. Det. Sgt. Darren Parisien of the Saskatoon Police Service Criminal Intelligence Section – Vice Unit discovered files containing child pornography by going on the internet and using the LimeWire file share program. He identified an IP address, being 70.64.12.102, as the source of some of the pornography that he located.

6. Det. Sgt. Parisien learned that the IP address in question was provided by Shaw Communications Inc. (“Shaw”). He was able to identify a globally unique identifier number (“GUID”) which would allow him to identify the particular computer that was being used to access the child pornography if it was located.

7. Det. Sgt. Parisien directed Sgt. Deb Altrogge of the Saskatoon Police Service to send a letter to Shaw seeking disclosure from that company of the identity and address of the subscriber of the said IP address.¹ Sgt. Altrogge advised Shaw that then Cst. Parisien was investigating a *Criminal Code* offence pertaining to child pornography on the internet. She requested the IP address pursuant to the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”), S.C. 2000, C.5. She stated that the information was requested to assist in an ongoing investigation and that Det. Sgt. Parisien had “the lawful authority to obtain the information” and that the request satisfied section 7(3)(c.1)(ii) of PIPEDA. The specific lawful authority was not identified nor was any explanation provided as to how the IP address in question related to the investigation.²

¹ Exhibit P-3, AR pages 123 to 128

² Exhibit P-3, AR pages 123 to 128

8. The letter was sent on September 4, 2007 and on September 10, 2007 Shaw, without any further inquiry, responded and advised that the subscriber of the IP address in question was the Appellant's sister and provided her address and phone number.³

9. Det. Sgt. Parisien maintained that he requested the information from Shaw pursuant to section 7(3)(c.1)(ii) of *PIPEDA*. He acknowledged that he could have obtained a judicial authorization to get this information from Shaw but he decided to simply make the request from the internet provider.

10. The Shaw privacy policy, which is found on its website, states "Shaw may disclose customer personal information to a third party or parties where the customer has given Shaw consent for such disclosure or if disclosure is required by law in accordance with the Personal Information Protection and Electronic Documents Act".⁴ Det. Sgt. Parisien was aware of this requirement.⁵ Det. Sgt. Parisien acknowledged that he did not know if the Appellant had ever received the policy.⁶ He equated obtaining the IP address to checking a license plate to determine a registered owner.⁷

11. The information obtained from Shaw was used by Det. Sgt. Parisien in an Information to Obtain and formed the basis for the search warrant which was issued pursuant to section 487 of the *Criminal Code* on September 20, 2007. The warrant was executed that day.

12. The Appellant was the sole resident of the premises that were searched. His computer was seized and it matched the GUID numbers that had earlier been identified.

13. Det. Sgt. Parisien acknowledged that he was aware of court decisions that went both ways in terms of the necessity for a judicial authorization to obtain an IP address from an

³ Exhibit P-3, AR pages 123 to 128

⁴ Exhibit P-8, AR pages 129 to 134

⁵ Preliminary Hearing Transcript ("PHT"), pages 34 to 37, questions 76 to 87

⁶ PHT, page 108, question 307

⁷ PHT, page 30, question 59

internet service provider.⁸ Nonetheless he proceeded to make the request of Shaw. He acknowledged that if Shaw had refused he would have applied for a production order or search warrant.⁹

14. Det. Sgt. Parisien agreed that Shaw was not required to give the police the information.¹⁰ He also acknowledged that he did not know whether the Appellant ever saw the Shaw privacy policy and while it changed from time to time the officer has always been aware of it.¹¹

15. There is no dispute that without the information obtained from Shaw there would not have been sufficient information to support the issuance of the search warrant.

C. Trial Judgment – *Voir Dire*

i) Section 8 Application

16. The Appellant brought a number of preliminary applications, including an argument that the obtaining of the IP address directly from Shaw without a prior judicial authorization was an unreasonable search and the evidence seized in the search should be excluded pursuant to section 24(2).

17. The trial judge determined that there was no expectation of privacy, either subjectively or objectively, concerning the IP address. He further stated that if there were any expectation of privacy this would be unreasonable in light of Shaw's Privacy Policy, its Accepted Use Policy and the power to disclose the IP address information pursuant to the provisions of PIPEDA.

D. Trial Judgment

i) *Mens Rea* Requirement of Section 163.1(3) of the *Criminal Code* – Making Available Child Pornography

18. Evidence was heard that the computer had accessed child pornography using the LimeWire program. This program does not have its own central database but rather draws from shared folders of other users. Similarly other users of the LimeWire program may draw from the

⁸ PHT, page 103, answer 392

⁹ PHT, pages 30 to 31, answer 60

¹⁰ PHT, page 105, answer 298

¹¹ PHT, page 107 to 108, answers 305 to 310

shared folder of the user's computer. The LimeWire program has a default setting that allows file sharing and unless it is purposely deactivated others may access data from the user's shared folder.¹²

19. The Appellant testified. The Crown also entered in evidence a statement that had been taken from him. The Appellant admitted that he understood that he was accessing and downloading images that contained child pornography. However, he stated that he did not understand that the LimeWire program permitted others to access the material in his shared file.¹³ He testified that he thought the material was derived from a central database.¹⁴ The Appellant maintained that he was not aware that the sharing function of the LimeWire program allowed others to access his computer until he was told by Det. Sgt. Parisien that he was going to be charged with "making available child pornography".¹⁵ The trial judge summarized his position as follows:

"In short, he disclaimed knowledge of the ability of LimeWire to give others access to his folder content".¹⁶

20. The Crown argued that the Appellant must have known of LimeWire's sharing capabilities by pointing to the program which referred to uploading rather than downloading, the home page that referred to the program as a "sharing program", the screen which indicated that it was sharing and the Appellant's testimony that he had used LimeWire for many years. The Crown argued that it was difficult to believe that the Appellant did not know the sharing function and that a reasonable inference could be drawn that he did know.

21. The trial judge considered the testimony of the Appellant and found that he was "thoughtful, not evasive and in my opinion his demeanor was consistent with someone telling the truth".¹⁷ He concluded that he believed the Appellant. He concluded that the offence requires proof that the Appellant "knowingly" committed the act alleged. He observed that two

¹² Trial Transcript ("TT"), pages 242-243.

¹³ TT, page 448.

¹⁴ TT, page 456.

¹⁵ TT, page 503

¹⁶ Trial Judgement ("TJ"), page 593

¹⁷ TJ, page 595

of the experts in computer science who testified for the Crown had gaps in their knowledge regarding computers and how particular programs functioned. He concluded that the Appellant did not have the “knowing, live intention to distribute”.¹⁸

22. In determining the requisite *mens rea* for section 163.1(3) of the *Criminal Code*, the trial judge noted that Parliament had drawn a distinction between possession and making available and that there was a significantly different minimum penalty for each. (In the case of possession a minimum sentence of 45 days while in the case of making available a minimum sentence of one year.) The trial judge observed that this Honourable Court in *R. v. Morelli*¹⁹ had determined that to be in possession meant to “knowingly be in possession”. On this basis he decided that to be guilty of making available child pornography an accused must do so knowingly.

23. The trial judge went on to then review the evidence and commented on what would be required for an accused to knowingly make available child pornography. He made reference to a positive step or action. In his judgment he then clarified what he meant. He described this as a “positive facilitation of the activity”.²⁰

24. In considering whether the accused made available child pornography he noted that there was no evidence that the accused had taken active facilitation steps that “would serve as an indicator of intent”.²¹ [emphasis added] In other words, a positive step would be evidence of, or would indicate knowledge. He did not state that it was a required element of knowledge.

25. The trial judge then went on to consider that the accused had used the LimeWire program and had not shut off the file sharing feature. He observed however that he was using the program simply as it was loaded with its default setting. In the circumstances he could not find that the accused had “... the knowing, live intention to distribute or make available ...”²² child pornography and dismissed the charge.

¹⁸ TJ, page 599

¹⁹ *R. v. Morelli*, 2010 SCC 8 [Morelli]

²⁰ TJ, page 597

²¹ TJ, page 599

²² TJ, page 599

E. The Court of Appeal Judgment

i) Search of Information Attached to IP Address – Section 8 Application

26. The Court of Appeal unanimously dismissed the Appellant's appeal but all three judges issued separate reasons. The principal reasons were found in the decision of Caldwell, J.A.

27. Caldwell, J.A. at the outset referred to the Saskatchewan Court of Appeal's companion decision in *R. v. Trapp*²³. There the police had obtained an IP address directly from SaskTel. The Court noted that in *Trapp*, because the provider of the information was a provincial company the *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 was applicable, as well as the SaskTel policy. In analyzing the question of the expectation of privacy, Caldwell, J.A. found the following:

- 1) There is a subjective expectation of privacy concerning the use by the Appellant of his computer in his home;²⁴
- 2) He agreed that determining the identity of the user of the computer would effectively reveal intimate details of the user;²⁵
- 3) He noted that the Appellant was not the subscriber but that would be the case in most homes as often there is only one subscriber with multiple users. Therefore, *prima facie*, the Appellant had a personal privacy right;²⁶
- 4) The Appellant was bound by the terms of the Shaw agreement and privacy policy and for this reason the Appellant's objective expectation of privacy was unreasonable;²⁷
- 5) He then reviewed the provisions of *PIPEDA* which allows the service provider to release information where there is informed consent and concluded that the Appellant's sister had given her express, informed consent when she subscribed for the internet service;²⁸

²³ *R. v. Trapp*, 2011 SKCA 143 [*Trapp*]

²⁴ Court of Appeal Judgment ("CAJ"), para. 17

²⁵ CAJ, para. 22

²⁶ CAJ, para. 27

²⁷ CAJ, para. 33

²⁸ CAJ, paras. 36 and 38

- 6) The Court determined that even if there were no informed consent the internet provider was entitled to release the information pursuant to the provisions of section 7(3)(c.1)(ii) of *PIPEDA*.²⁹

28. Section 7(3)(c.1)(ii) permits the disclosure of an individual's personal information to the police without the individual's knowledge or consent if the disclosure is:

(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

(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

29. Caldwell, J.A. determined that while the request didn't identify the lawful authority, it was made on the police letterhead. Also, it was not material in any event as the police had the authority to investigate.³⁰

30. He concluded that both the agreement with Shaw by the subscriber and *PIPEDA* gave Shaw the discretion to disclose and further that Shaw had the sister's expressed informed consent, all of which pointed to there being no reasonable expectation of privacy.³¹

31. Caldwell, J.A. then went on to hold that while the search was somewhat intrusive it was minimally so and if he was wrong in his determination of the issue of expectation of privacy the search was reasonable in any event.³²

32. Cameron, J.A. concurred in the result but found that there was an expectation of privacy, however he felt the search was reasonable.³³

²⁹ CAJ, para. 39

³⁰ CAJ, para. 40

³¹ CAJ, para. 42

³² CAJ, para. 43, 44 and 46

³³ CAJ, para. 98

33. Ottenbreit, J.A. found there was no expectation of privacy.³⁴

ii) Wilful Blindness

34. The Court of Appeal allowed the Crown's appeal. Caldwell, J.A. for the Court concluded that he was not supplanting the decision of the trial judge who found that the Appellant did not intend to share the files but concluded that the trial judge had erred by failing to consider whether or not the Appellant was guilty of wilful blindness.³⁵ He found that the trial judge had erred in holding that some active step was required to be guilty of making available child pornography.³⁶

35. Caldwell, J.A. reviewed the caselaw and the rules of statutory interpretation in concluding that the trial judge was correct that to be guilty of making available child pornography an accused must do so "knowingly". He then stated that the trial judge had determined that to knowingly make available child pornography "a positive step or action" was required.³⁷ He made this determination without any analysis of what the trial judge had actually said in determining the issue of *mens rea* or the specific findings involving the Appellant.

36. Caldwell, J.A. quoted from the debate in the House of Commons about the child pornography legislation. A review of the Justice Minister's comments indicates that whether the offence is possessing, accessing or making available, the accused must do so knowingly.³⁸

37. Without considering what the trial judge meant by a positive step or action, and specifically the trial judge's reference to this meaning that the accused had to "facilitate" access or that a positive step was an "indicator" of intent (ie. not an essential element), Caldwell, J.A. determined that the positive step referred to by the trial judge directly contradicted the stated intention and purpose of Parliament.³⁹ Based on this, Caldwell, J.A. then went on to consider whether or not wilful blindness would be sufficient to satisfy the *mens rea* element of making

³⁴ CAJ, para. 110

³⁵ CAJ, para. 91

³⁶ CAJ, para. 92

³⁷ CAJ, para. 73

³⁸ CAJ, para. 78

³⁹ CAJ, para. 81

available child pornography. He concluded that because the trial judge had erred in determining that a positive step was required he overlooked the issue of wilful blindness and as a result quashed the acquittal and ordered a new trial.⁴⁰

PART II – QUESTIONS IN ISSUE

38. It is respectfully submitted that the following are the issues to be considered by this Honourable Court:

Issue One: Was the Court of Appeal in error in determining that there was no reasonable expectation of privacy in the information attached to an IP address?

Issue Two: If the Appellant's rights under section 8 of the *Charter* were breached, should the evidence gathered upon the execution of the search warrant be excluded pursuant to section 24(2) of the *Charter*?

Issue Three: Did the Court of Appeal err in overturning the decision of the learned trial judge that the Appellant did not have the necessary *mens rea* to commit the offence of making available child pornography contrary to section 163.1(3) of the *Criminal Code* on the basis that he failed to consider the question of wilful blindness on the part of the Appellant?

PART III - STATEMENT OF ARGUMENT

Issue One: Was the Court of Appeal in error in determining that there was no reasonable expectation of privacy in the information attached to an internet protocol address?

A. The Nature of the Information Obtained

39. The fundamental error committed by Caldwell, J.A. was to not appreciate the significant impact of the disclosure of the subscriber information attached to an IP address on one's privacy rights. The internet has created an unusual situation where one can obtain a great deal of information about a particular user without identifying that individual. The individual's privacy rights are protected by anonymity. Once the individual's identity is provided his/her privacy rights are significantly infringed.

⁴⁰ CAJ, para. 92

40. The provision of a name and address without more would hardly be considered information for which there would be an expectation of privacy. However, when that information is provided in conjunction with a known IP address, the person receiving that information has access to a large trove of personal information for which there is a reasonable expectation of privacy.

41. This Honourable Court has on a number of occasions commented on the invasiveness and intrusiveness of one's privacy by the search of a seized personal computer. Fish, J. for the majority in *R. v. Morelli* recognized the privacy concerns, not only with medical and financial records and the like which might be stored on a computer, but also in determining where an individual had surfed on the internet:

[3] First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your e-mails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police 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.⁴¹ [emphasis added]

42. The determination of whether there is a subjective expectation of privacy must be answered in the context of the realities of our world. This Honourable Court recognized that technical differences inherent in new technology have to be recognized when assessing privacy rights. In that case the question was whether text messages fell outside the protection of private communications.⁴²

43. Virtually everything is done online, whether it is banking, booking an airline ticket, making an appointment to see a physiotherapist, communicating by e-mail or Facebook or simply surfing the internet. What once was safely locked away inside the confines of one's home now is found online. Where we have surfed on the internet reveals much about us and is

⁴¹ *Morelli*, *supra*, at para. 3

⁴² *R. v. TELUS Communications Co.*, 2013 SCC 16 at para. 5

information desired by many beyond the police agencies, including many arms of government and private industry as well. Are privacy interests to be compromised because virtually every segment of society now compels you to communicate, maintain records and conduct business in this fashion? Does it make any difference that in order to conduct one's affairs you have to secure the services of an internet provider? Would a citizen of Canada expect that their privacy interests should be compromised or indeed waived altogether simply because they are using the services of an internet provider?

44. The comments of McLachlin, C.J. and Fish, J. in *R. v. Gomboc*⁴³ are applicable to the case at bar.

[99] In our view, this appeal involves neither an isolated nor a *technical* matter regarding electrical consumption only. It raises core issues regarding the protection of privacy safeguarded by s. 8 of the *Charter*.

[100] Every day, we allow access to information about the activities taking place inside our homes by a number of people, including those who deliver our mail, or repair things when they break, or supply us with fuel and electricity, or provide television, Internet, and telephone services. Our consent to these "intrusions" into our privacy, and into our homes, is both necessary and conditional: necessary, because we would otherwise deprive ourselves of services nowadays considered essential; and conditional, because we permit access to our private information for the sole, specific, and limited purpose of receiving those services.

[101] A necessary and conditional consent of this sort 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 we watch on our television sets, what we listen to on our radios, or what we send and receive by e-mail on our computers.

45. The error of the Court of Appeal wasn't that it applied the wrong test but rather that it failed to appreciate the applicability of that test to online technology which challenges our conventional concepts of possession and privacy. As a society, we increasingly are forced to use online services, the scope and extent of which will undoubtedly be significantly expanded even by the time this appeal is argued.

⁴³ *R. v. Gomboc*, [2010] 3 SCR 211 at paragraphs 99 to 101 [*Gomboc*]

46. In examining this issue the majority in *R. v. Trapp*⁴⁴ agreed that when you subscribe for internet access service you do not surrender your expectation of privacy regarding what you choose to access on the internet. Cameron, J.A. relied on *R. v. Plant*⁴⁵ where Justice Sopinka stated:

[39] ...

Some indication of the parameters of the protection afforded by s. 8 with respect to informational privacy can be derived from the following passage from the reasons of La Forest J. in *Dyment*, [1988] 2 S.C.R. 417, at pp. 429-30, commenting on the Report of the Task Force on Privacy and Computers:

In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations about where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and *restricted to the purposes for which it is divulged*, must be protected. [emphasis added]

B. Section 8 Protected Privacy Interests

47. This Honourable Court identified three important privacy interests that require the protection of section 8, namely: personal privacy, territorial privacy and informational privacy.⁴⁶ It is common ground that what was being dealt with here is informational privacy.

48. In considering whether or not there is a reasonable expectation of privacy the court is required to assess the totality of the circumstances. Cory, J. in *R. v. Edwards*⁴⁷ identified a list of factors to be considered when making this assessment. This included:

- i) presence at the time of the search;
- ii) possession or control of the property or place searched;
- iii) ownership of the property or place;

⁴⁴ *Trapp*, *supra*, at para. 39

⁴⁵ *R. v. Plant*, [1993] 3 SCR 281 at para. 292 [*Plant*]

⁴⁶ *R. v. Tessling*, (2004) 3 SCR 432 at paras. 42 and 25

⁴⁷ *R. v. Edwards*, [1996] 1 SCR 128 at para. 45 [*Edwards*]

- iv) historical use of the property or item;
- v) the ability to regulate access, including the right to admit or exclude others from the place;
- vi) the existence of subjective expectation of privacy; and
- vii) the objective reasonableness of the expectation.

49. The totality of circumstances analysis was commented on further by this Honourable Court in *R. v. Patrick*⁴⁸ where Binnie, J. listed the following considerations:

- 1) What was the nature or subject matter of the evidence gathered by the police;
- 2) Did the (section 8 claimant) have a direct interest in the subject matter;
- 3) Did the (section 8 claimant) have a subjective expectation of privacy in the information contained in the subject matter;
- 4) If so, was the expectation objectively reasonable?

50. Caldwell, J.A. concluded that the first three criteria had been met noting that there was a subjective expectation of privacy concerning the use by the Appellant of his computer, that he had a direct interest in this notwithstanding that the internet service was subscribed for by his sister as it would be expected that other users in the home would be utilizing the service and that subjectively he would have expected this to be private. He concluded however that the Appellant failed on the fourth ground holding that in light of the terms of the Shaw agreement and privacy policy, as well as the provisions of *PIPEDA*, the expectation of privacy was not objectively reasonable. In this regard, notwithstanding that there was no direct evidence that the Appellant or his sister expressly consented to the release of the information by Shaw, or had ever even received the policies, he found that based on the terms of the Shaw agreement and privacy policy, which simply were posted on Shaw's internet website, that there was an express informed consent to the release of the information. Further, if the Appellant had a subjective

⁴⁸ *R. v. Patrick*, 2009 SCC 17 at para. 27

expectation of privacy as found by the Court of Appeal, would this not be in conflict with the suggestion that an expressed informed consent had been provided?⁴⁹

51. The Appellant submits that a posting by Shaw of the policies on a website falls far short of an express informed consent. It is true that the Appellant's sister had subscribed for the internet access. It is also true that there was no evidence that either she or the Appellant were aware of the policies. The standard of express informed consent is a high one. In *R. v. Rutten*⁵⁰ the court reviewed the requirements of a valid consent. The basic requirements were laid down by the majority of the Supreme Court of Canada in *R. v. Borden*⁵¹ where Iacobucci, J. in discussing a waiver of a right to be secure against an unreasonable seizure stated:

In order for a waiver of the right to be secure against an unreasonable seizure to be effective, the person purporting to consent must be possessed of the requisite informational foundation for a true relinquishment of the right. A right to choose requires not only the volition to prefer one option over another, but also sufficient available information to make the preference meaningful. This is equally true whether the individual is choosing to forego consultation with counsel or choosing to relinquish to the police something which they otherwise have no right to take.

52. Query whether Shaw even provided an informed consent to the disclosure of the information. The demand letter that was sent by the police to Shaw did not give Shaw any choice in the matter. Without identifying the particulars of why it was entitled to the information it demanded that it be produced. However, even if Shaw was consenting it had no authority to waive the Appellant's *Charter* rights. It could not any more legitimize the police seizure than could hotel clerks or landlords by unlocking a suite for the police without a warrant or a telephone service provider allowing police to listen in on telephone calls without authorization.

53. In determining the objective reasonableness of an expectation of privacy, Binnie, J. in *Patrick* set out a series of factors to be considered:⁵²

⁴⁹ CAJ, para. 17

⁵⁰ *R. v. Rutten*, 2006 SKCA 17 at para. 35

⁵¹ *R. v. Borden*, [1994] 3 SCR 145 at 162. See also *Korponay v. Canada (Attorney General)*, [1982] 1 SCR 41 at page 49

⁵² *Patrick*, *supra*, at para. 27

- a) the place where the alleged “search” occurred; in particular, did the police trespass on the Appellant’s property and, if so, what is the impact of such a finding on the privacy analysis;
- b) whether the informational content of the subject matter was in public view;
- c) whether the informational content of the subject matter had been abandoned;
- d) whether such information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality;
- e) whether the police technique was intrusive in relation to the privacy interest;
- f) whether the use of this evidence gathering technique was itself objectively unreasonable;
- g) whether the informational content exposed any intimate details of the Appellant’s lifestyle or information of a biographic nature.

54. Only when the analysis respecting the reasonable expectation of privacy is answered in the affirmative is it necessary to address the second question, namely: was the reasonable expectation of privacy violated by the police conduct (ie. was there an unreasonable search).

55. The jurisprudence in this area has been divided. In two of the first decisions,⁵³ the courts found that there was a reasonable expectation of privacy and that the “lawful authority” referred to in section 7(3)(c.1)(ii) referred to obtaining a search warrant. The court found that there had to be an independent overseer of the release of this private information identifying a subscriber and that the only reasonable party to carry out that role would be judicial authorization.

56. Other decisions have relied on the particular contractual arrangement that existed between the subscriber and the internet provider in holding that there was not a reasonable expectation of privacy.⁵⁴

⁵³ *Re S.C.* 2006 ONCJ 343 at paragraph 9 and *R. v. Kwok*, 2008 OJ No. 2414 at paragraph 35

⁵⁴ *R. v. Ward*, 2012 ONCA 660

i) Application of the Analysis to the Circumstances

a) The Subject Matter of the Search

57. It is incorrect to say that the only information being provided was the Appellant's sister's name and street address. In point of fact, the information provided by Shaw did two things:

- 1) It identified that not only the Appellant's sister but also anyone else residing with her, was using the IP address in question; and
- 2) Having identified who the subscriber was to that IP address it revealed a great deal of personal information about the people at that address. Knowledge that the user of that IP address had accessed different subject matters on the internet, gone to various websites and beyond, (the sky is the limit with the technology that is available) revealed "...biographical core data, revealing intimate and private information for which individuals rightly expect constitutional privacy protection".⁵⁵

b) The Appellant's Interest in the Subject Matter

58. Caldwell, J.A. recognized that for any household there is generally only one subscriber and then everyone in the household would access the internet through that one subscription.⁵⁶ In this case that is in fact what happened. For this reason the Appellant had an interest in the subject matter. Caldwell, J.A. rejected the Crown's submission that *R. v. Edwards*⁵⁷ stood for the proposition that the right to privacy is personalized, holding that *Edwards* did not support this narrow interpretation of section 8 of the *Charter*. He noted that Cory, J. relied on *R. v. Pugliese*⁵⁸ where Finlayson, J.A. stated:

When an accused, such as the appellant, asserts at his trial that there has been a breach of his s. 8 Charter right to be secure from unreasonable search or seizure, he is asserting a particular right to privacy which may, on occasion, be unrelated to any recognized proprietary or possessory right. Section 8 of the Charter is directed to the protection of the security of the person, not the protection of his property, and it is the appellant's personal exposure to the consequences of the

⁵⁵ *Gomboc, supra*, at para. 34

⁵⁶ CAJ, para. 23

⁵⁷ *Edwards, supra*, at para. 43

⁵⁸ *R. v. Pugliese*, (1992) 71 CCC (3d) 295 Ont.CA. at para. 11

search and seizure that gives him the right to challenge, not the search warrant itself, but the admission into evidence at his trial of the fact of the search and the account of what was seized.

59. The Appellant's subjective expectation of privacy was reasonable. It would be difficult to imagine that any reasonable person would think that the information that they have accessed over the internet and online would not have a subjective element of privacy. Caldwell, J.A. recognized this and took no issue with the Appellant's argument that he had a subjective element of privacy.

c) The Place Where the Alleged Search Occurred

60. The search ultimately occurred at the residence of the Appellant. This would be a strong indicator of a right of privacy. But even if one examines the question from the perspective that the seizure of the IP address was taken from the records of Shaw, the internet provider, still this would be a strong indicator of a right to privacy. Traditionally, the fact that the property was in the possession of a third party would mitigate against an expectation of privacy. That is no longer the case when an individual has no choice but to utilize the service of a third party internet provider who will have custody of their most private information. Similar to a situation where an individual rents a bus locker, which is not owned by him and for which the bus company has a master key, there still is a reasonable expectation of privacy.⁵⁹ An individual would expect the records of his internet provider and his identity to be kept confidential and private. Bearing in mind that disclosure of that information would have a significant impact on maintenance of the privacy of the individual subscriber, the public would have every reason to believe that the information would be kept private.

d) Was the Information in Public View

61. The information was not in public view. Unlike, for example, accessing a telephone number through directory assistance, this information was not accessible and not available for public view.

⁵⁹ *R. v. Buhay*, 2003 SCC 30 at paras. 22 to 24

e) Was the Information Already in the Hands of Third Parties and, if so, was it Subject to an Obligation of Confidentiality

62. Shaw had a privacy policy which is available for review on its website. There was no evidence that the Appellant or his sister were aware of the contents of that policy, that Shaw had reviewed that policy with them or obtained their expressed consent to the policy requirements.

63. Even at that the policy stated that it was “established ... in accordance with the *Personal Information Protection and Electronic Documents Act*” and which at paragraph 3.4.1 allows disclosure of personal information where “disclosure is required by law, in accordance with the *Personal Information Protection and Electronic Documents Act*”. Personal information according to the policy includes the customer’s name, address and phone number as set out in paragraph 3.1.1.⁶⁰ The policy is a reflection of what a subscriber would reasonably expect; their information would not be disclosed unless required by law. This contemplates something more than a police officer requesting the information. If that was all that was required there would be no protection whatsoever to an individual’s privacy rights. The gatekeeper that is required is judicial authorization to access the information.

64. In *Gomboc, supra*, this Honourable Court was dealing with the disclosure of electrical consumption rates. The majority noted that there was no statutory barrier to the utility provider’s voluntary cooperation with the police’s request and that express notice that such cooperation might occur existed. The majority noted that while this weighed heavily against giving the asserted expectation of privacy constitutional recognition, that this was not in and of itself determinative and that one must still proceed cautiously. Deschamps J. stated:

[33] ... 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.⁶¹

⁶⁰ Exhibit P-8, AR pages 129 to 134

⁶¹ *Gomboc, supra*, at para. 33

65. The “Joint Terms of Service” which is posted on Shaw’s website indicates that “Shaw may disclose any information as is necessary to: a. satisfy any legal, regulatory or other governmental requests; b. operate the Services properly; c. or protect Shaw or its customers, in accordance with the guidelines set out in Shaw’s Privacy Policy”.⁶² A plain reading of this would indicate that Shaw would only disclose information which was necessary/required to satisfy a government request. One might reasonably expect that Shaw would not provide a government agency one’s personal information unless it was required to do so, for example if the state agent had identified its legitimate lawful authority (eg. a search warrant).

66. Shaw also has as an “Acceptable Use Policy” posted on their website which describes the permitted uses of their services. Under the heading of “Violation of This Agreement” Shaw states that it does not routinely monitor the activity of accounts for violation of this agreement, but then indicates that it will respond to complaints it has become aware of. The document does state that “You hereby authorize Shaw to cooperate with (i) law enforcement authority in the investigation of suspected criminal violations; such cooperation may include Shaw providing a user name, IP address or other identifying information about a subscriber, in accordance with the guidelines set out in Shaw’s Privacy Policy”.⁶³ But again, it is reasonable to conclude that this simply means Shaw will not resist a valid search warrant, not that it will freely give out your information following a government request.

67. In Shaw’s Privacy Policy, which is also simply posted online, under the heading “Our Commitment to You” Shaw indicates “Shaw has always been and will continue to be committed to protecting personal information”.⁶⁴ The document then goes on to describe some of the principles which it has adopted with respect to privacy and personal information. Some of these principles include: identifying the purposes for personal information collection, obtaining consent, safeguarding personal information, and being open about policies and practices.

⁶² Exhibit P-8, AR page 135 to 143

⁶³ Exhibit P-8, AR pages 144 to 152

⁶⁴ Exhibit P-8, AR pages 129 to 134

68. At page 3 of Shaw's Privacy Policy it states: "Shaw generally seeks express consent when the Personal Information is likely to be considered sensitive. Implied consent is typically appropriate when the Personal Information is less sensitive".⁶⁵ We submit that given the breadth of the personal information available in this context, that express consent would be required and this would mean more than Shaw simply posting a notice on their website.

69. At page 4 of Shaw's Privacy Policy it states that "Shaw may disclose Customer's Personal Information to: (f) a third party or parties, where the Customer has given Shaw's Consent to such disclosure or if disclosure is required by law, in accordance with the *Personal Information Protection and Electronic Documents Act*".⁶⁶ [emphasis added] The phrase "required by law" supports the position that one's personal information would not be disclosed without judicial authorization.

70. The significant determining factor for the majority in *Gomboc* was that the DRA did not disclose intimate details of lifestyle and personal choice.⁶⁷ In the case of the Appellant, the policies of Shaw cannot be held to determine the issue bearing in mind the intimate details of lifestyle and personal choice that it discloses. The intimate and personal nature of the information dictates that the privacy rights of the Appellant must prevail.

71. The Crown relies on section 7(3)(c.1)(ii) of *PIPEDA*, arguing that they had "lawful authority" to obtain the records. Caldwell, J.A. states that the lawful authority flowed from the general investigative powers of the police. In other words, the police were obligated to investigate possible *Criminal Code* offences and in doing so could request information.

72. He found support for this in the production provisions found in section 487.014(1) of the *Criminal Code*. Applying that reasoning there would never be any need for search warrants or wiretap authorizations as the police could always state that they were simply obtaining the information in furtherance of a lawful investigation. In reality, such a request must be tempered by the fact that if provision of the requested information would involve an invasion of a person's

⁶⁵ Exhibit P-8, AR pages 129 to 134

⁶⁶ Exhibit P-8, AR pages 129 to 134

⁶⁷ *Gomboc*, *supra*, at para. 50

privacy then appropriate judicial authorization, whether by way of a search warrant or a production order, must be obtained.

73. In the case at bar the bare demand stated that the Saskatoon Police Service was investigating a child pornography matter and that it was asking for an IP address. No connection was disclosed between the IP address and the investigation nor any basis for believing that disclosure of information about the IP address would be relevant to the investigation. It would not have been appropriate for a Justice of the Peace to have issued a production order or authorized a search warrant based solely on this information.

74. *PIPEDA* was passed not to enhance the power of the state to intrude into our private lives but rather to protect privacy rights. The *Act* is preceded with the description that it is “...to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances...” [emphasis added]. That purpose is codified in section 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. ...”

75. The purpose of *PIPEDA* is not to enhance police powers but rather to protect privacy rights. Concerning requests for disclosure of personal information by government institutions, such as the Saskatoon Police Service, lawful authority is required. Because of the nature of the information requested the only reasonable lawful authority would be judicial authorization. This section would otherwise have the effect of giving the police a general investigative power to collect intimate and revealing personal information without any judicial oversight. *PIPEDA* does not lend support for the police or the internet provider’s conduct in this case. Rather, it supports the position that the provision of the information represented an unreasonable search.

76. It is important to keep in mind that the Appellant is not arguing that the police did not have the right to try and obtain the information. They did. But in order to maintain some control over this conduct it is reasonable that they be required to obtain judicial authorization. In this case the police wrote to Shaw, giving only a vague reference to an investigation regarding child pornography. No specifics were given with respect to their grounds for the belief that the subscriber had downloaded child pornography. For all Shaw knew at the time, this “investigation” may have simply involved the random selection of IP addresses by police. Most troubling is that a letter like this could apply to any number of broad-based investigations and Shaw would have provided the information without question.

f) Was the Police Technique Intrusive in Relation to the Privacy Interest?

77. The Supreme Court of Canada in *R. v. Plant*⁶⁸ some 20 years ago recognized that invasion by state agents in personal computer records confidentially maintained by a private citizen would be intrusive. The scope of information that would be available on an individual’s computer today likely was not even remotely contemplated by this Court in 1993. Today, determining the IP address allowed the state to access personal information about the Appellant. Without the information that was provided by Shaw no such intrusion could have taken place. Caldwell, J.A. found that the search was intrusive, although minimally so. Providing an individual’s address and phone number would be minimally intrusive. Determining where a particular subscriber has surfed on the internet and then obtaining that information which would identify that specific subscriber is significantly intrusive.

g) Was the Evidence Gathering Technique Itself Objectively Unreasonable?

78. Det. Sgt. Parisien knew that he was operating in a gray area. He knew that he had the ability to apply for a judicial authorization. Nonetheless without identifying his lawful authority he made a bare request to Shaw for the information. Shaw did not ask what the basis was for the lawful authority. Instead, Shaw did exactly what it was told to do. It bowed to the demand of the state without question. Perhaps the thought that it might be seen as aiding those accessing child pornography was the compelling reason to comply with the request without any

⁶⁸ *Plant, supra*

inquiry. There were no exigent circumstances and no reason why a judicial authorization couldn't have been sought. Without the benefit of some sort of judicial oversight, how often would personal information like this be requested and provided without question? How often would it be done without the user even being aware that it was taking place? In the circumstances the technique itself was objectively unreasonable.

79. Caldwell, J.A. in his decision cited Professor Quigley's work, *Procedure in Canadian Criminal Law*, 2nd Edition (Toronto: Carswell, 2005) to indicate that the police are entitled to ask individuals questions or make other inquiries during the process of investigating a crime. He notes that Professor Quigley indicates that "Historically, these situations, which are very frequent in the investigation of crime, have required no legal regulation because the law has presumed the conversations to be voluntary and consensual, except where the voluntary confession rule comes into play".⁶⁹ However, Professor Quigley cautions readers that many individuals will speak to the police out of respect or fear for authority rather than out of a desire to be of assistance. Professor Quigley in his work goes on to say:

At one time consent to police authority was a very broad concept based on the tort principles of *volenti non fit injuria*. An individual who consented to police authority thereby waived any redress against or legal protection from police intrusions on his liberty. However, unlike tort law, there was little discussion in criminal cases about the need for consent to be predicated upon sufficient information to assess one's legal rights.

This changed with the Supreme Court decision in *Dedman v. R.*, where it was recognized that mere acquiescence or compliance with police direction should not be equated with consent. To constitute valid consent to police authority, there must be a clear indication from the police that there is a choice whether or not to follow the direction. As twin bases for construing consent narrowly, the Court rightly pointed to the inherently intimidating nature of police action plus the difficulty for the public to ascertain the precise extent of police powers. Because consent to police authority is a form of waiver, it is also no accident that the Court framed consent in terms very similar to the doctrine of waiver in *Charter* jurisprudence. Although *Dedman* was a non-*Charter* case, its approach to consent has been adopted in the *Charter* era.

⁶⁹ *Procedure in Canadian Criminal Law*, 2nd Edition (Toronto: Carswell, 2005) at p. 5-2

80. The fact of the matter is that when the police demand information and state that they have “lawful authority” and are investigating a case of child pornography, it would be difficult to imagine any internet provider refusing to comply with the request. The courts have recognized “the authoritative and coercive character of police requests” and “the intimidating nature of police action and uncertainty as to the extent of police powers”.⁷⁰ What internet provider in the face of such a demand, especially as soon as the words “child pornography” are contained in the demand, would refuse to disclose the information.

81. In the case at bar, the letter provided to Shaw from the police seems to indicate that the company has no choice but to provide the documents. This is precisely the type of situation which Professor Quigley was alluding to.

h) Does the Information Reveal Intimate Details of the Appellant’s Lifestyle or Biography?

82. Knowing what a specific individual has accessed on the internet does reveal intimate details of the Appellant’s lifestyle or biography. Whether the information involved seeking out a divorce lawyer, Swiss banking instructions, self-defence techniques, inquiries about a specific company or business or political views or lifestyle choices (both legal and illegal), all reveal intimate details.

ii) Totality of the Circumstances

83. In looking at the totality of the circumstances there was an objective expectation of privacy. Users of the internet reasonably expect to be able to work under relative anonymity. While the internet can be used for illegal purposes, the Appellant’s position will ensure that a neutral gatekeeper will decide when the state should be able to obtain the information in question. In “Legal Issues in Anonymity and Pseudonymity”, A. Michael Frommkin identified the issues as follows:

“... The Internet is often seen as an anarchic medium. Ironically, fully traceable Internet transactions, not to mention traceable Internet communication, might mean that the Internet could become the foundation of the opposite of anarchy: a

⁷⁰ *Dedman v. The Queen et al*, [1985] 2 SCR 2 at paras. 9 to 10, 16 to 17, *R. v. Therens et al*, [1985] 1 SCR 613 at 644, *R. v. Woods*, 2004 MBCA 46 at para. 31 and *R. v. Woods*, 2005 SCC 42

life in which data recording everyone's movements, tastes, purchases, medical history, reading habits, and contacts with officialdom are commodified and available to some, and perhaps even to all. If so, then anonymous communications will be critical to the preservation of personal privacy."

84. We are obligated to use online services for virtually every aspect of our daily life. This fact has resulted in significant encroachment on our personal privacy. Imposing the obligation on the state to obtain judicial authorization to secure the subscriber information attached to an IP address creates a very insignificant obligation on the state that has far reaching implications on the efforts of individuals to maintain their privacy. The comments by this Honourable Court in *R. v. Duarte*⁷¹ are applicable. La Forest, J. stated:

[40] Harlan J. went on to make the seminal observation that the imposition of a warrant requirement would have the sole effect of ensuring that police restrict "participant monitoring" to cases where they can show probable cause for a warrant. It is unclear to me how compelling the police to restrict this practice to instances where they have convinced a detached judicial officer of its necessity would hamper the police's ability effectively to combat crime. But even if this were so, this restriction would be justified by the knowledge that the police would no longer have the right "to train these powerful eavesdropping devices on you, me, and other law-abiding citizens as well as the criminal element", to cite the observation of Cirillo J. in *Commonwealth v. Schaeffer*, supra, at p. 367. The appellant put the matter trenchantly in his factum:

A warrant requirement simply ensures that when the undercover agent goes in with the potential to make a permanent, electronic record of the conversation that takes place, it will be one that should be recorded (a proposed drug sale), as opposed to one that should not (the suspect's sex life or his views of the government).

85. Similarly in *R. v. Wong*⁷², this Honourable Court emphasized the need to take an objective view of the question that one is asking. In *Wong* this Court was dealing with the privacy interest in hotel rooms. *Wong* would suggest that we should not ask whether a suspected child pornographer has a reasonable expectation of privacy but rather we should ask a "neutral question" as to whether an internet user has a reasonable expectation of privacy?

⁷¹ *R. v. Duarte*, [1990] 1 SCR 30 at p. 52 to 53

⁷² *R. v. Wong*, [1990] 3 S.C.R. 36

86. Expecting the service provider to exercise “a meaningful measure of independent and informed judgment” in deciding whether to make the full disclosure requested by the police which was relied upon by Cameron, J.A. in *R. v. Trapp*, *supra*, and the Ontario Court of appeal in *R. v. Ward*⁷³ is not reasonable. The internet service provider in the face of a request from the state is not the type of independent judicial authority that should be making that determination. This is best illustrated by the facts of this case where Shaw complied, without question, to a request for the subscriber information attached to an IP address, which did not identify a lawful authority or outline any connection between this particular IP address and child pornography.

87. In conclusion, after analyzing the facts of this particular case and applying the criteria as outlined by this Honourable Court, the Appellant had both a subjective and objective expectation of privacy. The Saskatchewan Court of Appeal erred in its determination to the contrary.

iii) Was the search reasonable?

88. Caldwell, J.A. relied on the reasoning of Cameron, J.A. in *R. v. Trapp*, *supra*, in determining that the search was reasonable.⁷⁴ As in *Trapp*, he found that the “search” was authorized by law, the law was reasonable and that the manner in which the search was conducted was reasonable.

89. For the reasons outlined above, we submit that the search was not authorized by law. Section 487.014(1) did not authorize Shaw to release the information nor did the provisions of *PIPEDA*. Secondly, the search was not carried out in a reasonable fashion. Det. Sgt. Parisien knew that he was operating in a gray area but even then did not comply with the provisions of *PIPEDA* by disclosing his alleged lawful authority to demand the information from Shaw. Finally, because there was a reasonable expectation of privacy and this was a warrantless search it was *prima facie* unreasonable.⁷⁵

⁷³ *R. v. Ward*, 2012 ONCA 660 at para. 105

⁷⁴ CAJ, para. 46

⁷⁵ *Hunter v. Southam Inc.*, [1984] 2 SCR 145 at 161

Issue Two: If the Appellant's rights under section 8 of the *Charter* were breached, should the evidence gathered upon the execution of the search warrant be excluded pursuant to section 24(2) of the *Charter*?

90. Having determined that there was an unreasonable search and seizure, applying the considerations outlined by this Honourable Court in *R. v. Grant*, the evidence should be excluded.⁷⁶ The information associated with the IP address was the cornerstone of the search warrant application. Without it there was no basis to issue the search warrant and as a consequence any of the material seized in the search of the Appellant's premises, including his computer and its contents, should be excluded.

A. The Seriousness of the *Charter* Infringing State Conduct

91. Here the information obtained led to the disclosure of intimate details about the individual. This was a warrantless search. The breach was serious in that Det. Sgt. Parisien knew he was operating in a gray area, he knew he could apply for judicial authorization and he knew that there was nothing urgent that would prevent him from applying for that authorization. Nonetheless he went ahead with the demand and even then did not comply with the provisions of *PIPEDA* by outlining his lawful authority. In the circumstances the breach was serious.

B. The Impact of the *Charter* Protected Interests of the Appellant

92. As noted by Fish, J. in *R. v. Morelli*:⁷⁷

... it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical and personal situations. They even reveal our specific interests, like, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.

93. The impact in this case was significant. Even if a resulting search of the computer did not take place and all that the provision of the subscriber information for the IP address did

⁷⁶ *Morelli, supra*, at para. 11, and 98-113; *R. v. Grant*, 2009 SCC 2 at para. 72

⁷⁷ *Morelli, supra*, at para. 105

would be to identify the activities of the user on the internet, the impact on the Appellant's *Charter* protected interests would be significant. Det. Sgt. Parisien testified that he was able to access the information using a publicly available computer program. All that he was missing was the identity of the holder of the IP address. Disclosure of that information defeated the only privacy protection one has with the internet: anonymity. The provision of this information which determined the identity of the user of this IP address represented a significant intrusion of the *Charter* protected privacy interests of the Appellant.

C. Society's Interest in Adjudication on the Merits

94. While it is acknowledged that the exclusion of the evidence will significantly impact on the Crown's case, the importance of excluding the evidence in these circumstances far exceeds the need for the Crown to successfully proceed with this prosecution. If the evidence is not excluded then there effectively will be no oversight to the state's continuing access to this most private information without establishing any reasonable criteria for same. As we move towards a time when virtually every aspect of our personal life is found on our computer, the need for judicial authorization to access that information is more important than ever. As noted by Fish, J. in *R. v. Morelli*:

[111] The public must have confidence that invasions of privacy are justified, in advance, by a genuine showing of probable cause. ...⁷⁸

95. Fish, J. in *Morelli* commented on the particularly insidious nature of child pornography and the wide-spread condemnation and intense feelings of disapprobation if not revulsion that it generates but he noted that it is for this reason that the courts:

... must be particularly vigilant to issue process, or subsequently validate the issuance of process, only where reasonable and probable grounds for a search or an arrest are in fact made out. While the law must be relentlessly enforced, legal requirements must be respected, and constitutional safeguards preserved.⁷⁹

96. In the case at bar, the police did not comply with even the minimal safeguards of identifying to the service provider the particular lawful authority or basis for their demand.

⁷⁸ *Morelli, supra*, at para. 111

⁷⁹ *Morelli, supra*, at para. 9

Because the Court of Appeal ruled that no prior judicial authorization was required there is effectively no gatekeeper to ensure that one's *Charter*-mandated privacy rights are protected. It is for these reasons that admitting the evidence would bring the administration of justice into disrepute.

Issue Three: Did the Court of Appeal err in overturning the decision of the learned trial judge that the Appellant did not have the necessary *mens rea* to commit the offence of making available child pornography contrary to section 163.1(3) of the *Criminal Code* on the basis that he failed to consider the question of wilful blindness on the part of the Appellant?

A. The Decision of the Court of Appeal

97. The Court of Appeal eventually determined that to be guilty of making available child pornography the *mens rea* element included the requirement that this was done “knowingly”. Bearing in mind there was nothing in the legislation that suggested otherwise and a conviction would result in a mandatory minimum one year jail sentence, no other conclusion was possible. The Court of Appeal then erred in its analysis of the wilful blindness issue. In this regard it made two errors:

- 1) The Court of Appeal determined that the trial judge had decided that a positive step or action “was required in order to establish that an accused knowingly made child pornography available”. There was no analysis of the trial judge’s decision in this regard. Had the Court reviewed the trial judge’s decision in its entirety it would have been clear that the trial judge was simply ruling that to be guilty of knowingly making available, the accused would have to direct his mind in a positive way to the issue of whether or not child pornography was being distributed to others. His reference to the requirement that the accused facilitate the distribution made it clear that he was referring to either actively taking a step to distribute or being aware that by his lack of action he was distributing pornography and deciding to proceed in any event. Any confusion over that interpretation by the trial judge was resolved when he stated in his decision that evidence of a positive step would be “an indicator” that the accused had the

required *mens rea*. He did not state that it was a required element but only a factor to be considered in the evidence;

- 2) Caldwell, J.A. expressly stated that he was not supplanting the findings made by the trial judge⁸⁰, but that is exactly what he did. The trial judge found that the “true awakening” as described by Caldwell, J.A. had not occurred.⁸¹ Once the trial judge had determined that the Appellant did not know that he was sharing files with others and in fact thought that what was being accessed was through a central server, there was no longer any basis to determine that he was guilty of wilful blindness.

B. Positive Step or Action

98. Caldwell J.A. found “in my view the trial judge erred in his determination that the plain meaning of s.16.1(3) required a positive step to make available child pornography because that requirement is neither confirmed nor ruled out on the plain meaning of the section”.⁸² He found that “The plain meaning of the text, in its grammatical and ordinary sense, is it is a crime to do anything which disseminates or facilitates the dissemination of child pornography”.⁸³ This latter finding is largely correct; however the act or omission which facilitates the dissemination of child pornography must be done *knowingly* in order for it to constitute an offence.

99. Caldwell, J.A. misinterpreted the trial judge’s findings with respect to the use of the phrase “positive step” by taking it out of the context in which it was said, and by failing to appreciate the role of that phrase in the judgment in its entirety. Again, he was largely correct in finding, “if an overt act or positive step is required, that requirement is satisfied by an accused downloading child pornography using a file sharing program which makes it publicly available as a shared file”.⁸⁴ This is not disputed, however as with the above, this statement is only correct with the added caveat that the trier of fact must be satisfied beyond a reasonable doubt that the accused *knew/had actual or imputed knowledge* that the files were being made available.

⁸⁰ CAJ, para. 91

⁸¹ CAJ, para. 87

⁸² CAJ, para. 73

⁸³ CAJ, para. 70

⁸⁴ CAJ, page 80

100. The trial judge stated the law clearly and correctly when he found that the words used in s. 163.1(3), “all bear a connotation of a positive facilitation of the activity.”⁸⁵ Here he clarified that a positive step meant that the offence requires “positive facilitation.” This is a much broader interpretation than is alluded to by Caldwell, J.A.

101. The trial judge went on to find that, “A positive action of some kind appears to be contemplated by the legislature or the Parliament in order for the action to raise to a level which is generally classifies as distribution. . .”.⁸⁶ He does not limit this positive action to anything in particular, and the Appellant submits that this positive action could be established where an accused downloaded child pornography using a file sharing program, provided that the accused does so knowing that it is facilitating its distribution. By the trial judge’s own findings no other positive step than that would be required: “Thus the question that I must answer is did Mr. Spencer knowingly distribute by making available child pornography to others at that level of offence.”⁸⁷ He does not limit the question by imposing the requirement of an explicit positive step.

102. Caldwell J.A. concluded at paragraph 81 that, “the *mens rea* of the offence of making available child pornography under s. 163.1(3) is satisfied where an accused has downloaded child pornography or otherwise made child pornography available to others via a file sharing program over the internet. No other steps or actions to distribute it are required and the trial judge committed a substantive error of law when he concluded otherwise”.⁸⁸ This is incorrect. Section 163.1(3) is not a strict liability offence, and as such it is not enough for the Crown to simply establish that an accused has downloaded child pornography using a file sharing program. The Crown must prove beyond a reasonable doubt that the accused actually knew that he was sharing these files over the internet. Being reckless in this regard is not sufficient; the accused must have actual knowledge.

⁸⁵ TJ, page 597

⁸⁶ TJ, page 597

⁸⁷ TJ, page 598

⁸⁸ CAJ, para. 81

103. Caldwell, J.A. goes on to find that, “In the context of a file sharing program, the *mens rea* element of making available child pornography under s. 163.1(3) requires proof of the intent to make computer files containing child pornography available to others using that program or actual knowledge that the file sharing program makes files available to others”.⁸⁹ [emphasis added] This is correct, and it is precisely what the trial judge was referring to when he used the phrase “positive step”. The trial judge did not find that a positive step was a required element of the offence, but rather he found, “In this case Mr. Spencer did not take active facilitation steps that would serve as an indicator of intent.”⁹⁰ [emphasis added]

104. With respect to the proof of intent, the trial judge found, “He did not characterize the material so as to assist the LimeWire program. True, he did not shut off the default setting, but then again, this was not a positive act, he just used the program as it was loaded.”⁹¹ The trial judge did not indicate that to be guilty of this offence an accused *must* perform a positive act, rather he considered the evidence of intention/knowledge. He noted that the default setting was not changed, simply to comment on the lack of evidence in this regard. Had the Appellant performed a positive act such changing the program from a default setting where it did not share, to one where it did share, then that would be evidence of the intention to make child pornography available to others. It is not a requirement of the offence, but it would be proof of an accused’s intention.

C. Wilful Blindness

105. Caldwell, J.A. then held that because the trial judge had mistakenly found that there had to be a positive step, he failed to consider the question of wilful blindness. Wilful blindness was no longer a consideration once the Appellant testified that not only did he not know that his files were available to other LimeWire subscribers but that he mistakenly understood that when he was using the LimeWire program he was accessing information from a central mainframe, in other words that *his* files were not being shared.⁹² Once that testimony of the Appellant was

⁸⁹ CAJ, para. 87

⁹⁰ TJ, page 599

⁹¹ TJ, page 599

⁹² TT, pages 448, 456-458.

found to have at least raised a reasonable doubt and was not rejected there was no longer any room for consideration of the issue of wilful blindness.

i) The Law Regarding the Doctrine of Wilful Blindness

106. Caldwell, J.A. in his decision cited the seminal decision of the Supreme Court in *R. v. Sansregret* and quotes from that decision:

Wilful blindness is distinct from recklessness because, while recklessness involves knowledge of a danger or risk and persistence in a course of conduct which creates a risk that the prohibited result will occur, wilful blindness arises where a person who has become aware of the need for some inquiry declines to make the inquiry because he does not wish to know the truth. He would prefer to remain ignorant. The culpability in recklessness is justified by consciousness of the risk and by proceeding in the face of it, while in wilful blindness it is justified by the accused's fault in deliberately failing to inquire when he knows there is reason for inquiry.⁹³

The Court in *Sansregret* went on to find:

The textwriters have also dealt with the subject, particularly Glanville Williams (*Criminal Law: The General Part*, 2nd ed. 1961, at pp. 157-160). He says, at p. 157:

Knowledge, then, means either personal knowledge or (in the licence cases) imputed knowledge. In either event there is someone with actual knowledge. To the requirement of actual knowledge there is one strictly limited exception. Men readily regard their suspicions as unworthy of them when it is to their advantage to do so. To meet this, the rule is that if a party has his suspicion aroused but then deliberately omits to make further enquiries, because he wishes to remain in ignorance, he is deemed to have knowledge.

...

Glanville Williams, however, warns that the rule of deliberate blindness has its dangers and is of narrow application. He says, at p. 159:

The rule that wilful blindness is equivalent to knowledge is essential, and is found throughout the criminal law. It is, at the same time, an unstable rule, because judges are apt to forget its very limited scope. A court can properly find wilful blindness only where it can almost be said that the defendant actually knew. He suspected the fact; he realized probability; but he refrained from obtaining the final confirmation because he wanted in the event to be able to deny knowledge. This, and this alone, is wilful blindness. It requires in effect a finding that the defendant intended to

⁹³ *R. v. Sansregret*, [1985] 1 S.C.R. 570; 17 D.L.R. (4th) 577 at 584 to 586 [*Sansregret*]

cheat the administration of justice. Any wider definition would make the doctrine of wilful blindness indistinguishable from the civil doctrine of negligence in not obtaining knowledge. [emphasis added]

107. The doctrine of wilful blindness is an especially narrow rule. Evidence of its limited application can be found in the facts of *Sansregret* itself. That case involved two separate incidents where an accused broke into the home of the complainant, and after confining her and tying her up, she “consented” to sexual activity out of fear for her safety. Two of these incidents occurred, one in September, the other a month later in October. The Court found:

This case reveals, in my view, an appropriate set of circumstances for the application of the ‘wilful blindness’ rule. I have outlined the circumstances which form the background. I have referred to the findings of the trial judge that the appellant blinded himself to the obvious and made no inquiry as to the nature of the consent which was given. If the evidence before the Court was limited to the events of October 15, it would be difficult indeed to infer wilful blindness. To attribute criminal liability on the basis of this one incident would come close to applying a constructive test to the effect that he should have known she was consenting out of fear. The position, however, is changed when the evidence reveals the earlier episode and the complaint of rape which it caused, knowledge of which, as I have said, had clearly reached the accused. Considering the whole of the evidence then, no constructive test of knowledge is required. The appellant was aware of the likelihood of the complainant’s reaction to his threats. To proceed with intercourse in such circumstances constitutes, in my view, self-deception to the point of wilful blindness.⁹⁴

108. In *R. v. Jorgensen*⁹⁵, Sopinka, J. stated:

The second response to the concerns expressed by the Crown relates to the principles of wilful blindness. It is well established in criminal law that wilful blindness will also fulfil a mens rea requirement. If the retailer becomes aware of the need to make further inquiries about the nature of the videos he was selling yet deliberately chooses to ignore these indications and does not make any further inquiries, then the retailer can be nonetheless charged under s. 163(2)(a) for “knowingly” selling obscene materials. Deliberately choosing not to know something when given reason to believe further inquiry is necessary can satisfy the mental element of the offence.

...

⁹⁴ *Sansregret*, *supra*, at 586 to 587

⁹⁵ *R. v. Jorgensen*, [1995] 4 S.C.R. 55 at para. 102

As Glanville Williams wrote in *Criminal Law: The General Part* (2nd ed. 1961), at pp. 157-58:

[T]he rule is that if a party has his suspicion aroused but then deliberately omits to make further enquiries, because he wishes to remain in ignorance, he is deemed to have knowledge. . . .

. . . In other words, there is a suspicion which the defendant deliberately omits to turn into certain knowledge. This is frequently expressed by saying that he "shut his eyes" to the fact, or that he was "wilfully blind".

And, at pp. 158-59, the learned author states:

Before the doctrine of wilful blindness applies, there must be realisation that the fact in question is probable, or, at least, "possible above the average". . . . [emphasis added]

109. More recently in *R. v. Briscoe*,⁹⁶ this Honourable Court affirmed this interpretation of the doctrine of wilful blindness:

Wilful blindness does not define the *mens rea* required for particular offences. Rather, it can substitute for actual knowledge whenever knowledge is a component of the *mens rea*. The doctrine of wilful blindness imputes knowledge to an accused whose suspicion is aroused to the point where he or she sees the need for further inquiries, but *deliberately chooses* not to make those inquiries. See *Sansregret v. The Queen*, [1985] 1 S.C.R. 570, and *R. v. Jorgensen*, [1995] 4 S.C.R. 55. As Sopinka J. succinctly put it in *Jorgensen* (at para. 103), "[a] finding of wilful blindness involves an affirmative answer to the question: Did the accused shut his eyes because he knew or strongly suspected that looking would fix him with knowledge?"

In that case this Honourable Court found:

Professor Don Stuart makes the useful observation that the expression "deliberate ignorance" seems more descriptive than "wilful blindness", as it connotes "an actual process of suppressing a suspicion". Properly understood in this way, "the concept of wilful blindness is of narrow scope and involves no departure from the subjective focus on the workings of the accused's mind" (*Canadian Criminal Law: A Treatise* (5th ed. 2007), at p. 241). While a failure to inquire may be evidence of recklessness or criminal negligence, as for example, where a failure to inquire is a marked departure from the conduct expected of a reasonable person, wilful blindness is not simply a failure to inquire but, to repeat Professor Stuart's words, "deliberate ignorance".⁹⁷

⁹⁶ *R. v. Briscoe*, 2010 SCC 13; [2010] 1 S.C.R. 411 at para. 21 [*Briscoe*]

⁹⁷ *Briscoe*, *supra*, at para. 24

110. The Ontario Court of Appeal in *R. v. Smith*⁹⁸ summarized the issue succinctly:

We think both courts erred in law in the application of the wilful blindness doctrine. Wilful blindness requires more than a failure to make inquiries where those inquiries could have been made and reasonably should have been made by the accused. Wilful blindness requires a finding that the accused, knowing he had reason to suspect that a certain state of affairs existed, deliberately declined to make the inquiries necessary to confirm that state of affairs preferring instead to remain ignorant of the true state of affairs. This is a subjective state of mind and justifies the imposition of criminal culpability: see D. Stuart, *Canadian Criminal Law* (4th ed.) at pp. 228-31; *R. v. Rashidi-Alavije* 2007 ONCA 712 at paras. 22-24 (C.A.). [emphasis added]

111. In summary, wilful blindness is to be applied only where:

- 1) The accused has become aware of the fact, and the need to make further inquiry but deliberately closes his eyes to the issue;
- 2) This realization must be more than a mere suspicion. The accused must realize that the particular state of affairs is probable;
- 3) This must be proven to be a subjective state of mind. It must be proven to be deliberate ignorance;
- 4) The knowledge should only be imputed where it can almost be said that the accused had actual knowledge;
- 5) It is not enough that the accused ought to have made the inquiries, or a reasonable person would have made those inquiries; and
- 6) In effect it requires a finding that the accused intended to cheat the administration of justice, and in that regard would require some evidence that the accused would have benefited from purposefully remaining ignorant.

ii) Application to the Case at Bar

112. The trial judge summarized the Appellant's position as follows:

⁹⁸ *R. v. Smith*, 2008 ONCA 101; [2008] O.J. No. 465 [*Smith*] at para. 5

Mr. Spencer's position, in his videoed statement, his trial evidence, and through his counsel's submission, was that it was not until he was advised by Mr. Parisien that the alleged offences against him included possession and "make available" that he realized or apparently became aware that the LimeWire program he was using made the pornographic images held in his shared folder, available to others with no separate action on his part.

...

He says that he believed the images that he obtained came from a central database, not from a database which included his shared folder. In short, he disclaimed knowledge of the ability of LimeWire to give others access to his folder content.⁹⁹ [emphasis added]

113. The trial judge found the Appellant to be, "thoughtful, not evasive, and in my opinion his demeanor was consistent with someone telling the truth."¹⁰⁰ The trial noted the Appellant's apparent surprise to the revelation that he was being charged with making available when he stated in the interview, "I know I possessed, why mention make accessible?"¹⁰¹ The trial judge reflected on this and posed the question to be answered this way: "Was this a fiction or a true awakening to what the nature of the offence he was charged with."¹⁰² The phrase "true awakening" indicates that the trial judge was alive to the issue of wilful blindness and the possibility that this was not the first time the accused had considered this. Having determined that the evidence of the Appellant at the very least raised a reasonable doubt, he could not reject the finding that this was a true awakening and thus wilful blindness had no application.

114. The trial judge referred to the case of *R. v. Johansson*¹⁰³ which had just recently been decided at the time. The facts in that case were similar, and also involved the use of the program LimeWire. The trial judge distinguished that case from the case at bar, stating:

Justice Gabrielson did not believe the accused in that case. He stated:

The accused is not credible. He gave his testimony in a very quiet and somewhat hesitant fashion. I had to ask him on several times to speak up,

⁹⁹ TJ, page 593

¹⁰⁰ TJ, page 595

¹⁰¹ TJ, page 598

¹⁰² TJ, page 598

¹⁰³ *R. v. Johansson*, 2008 SKQB 451

so he could be heard. On occasion he would deny knowledge of the matters, that when confronted with the documents, he then acknowledged he may have known. His body language also displayed a nervous and anxious individual, not consistent with a truthful witness.¹⁰⁴

115. The description of the witness in *Johannson* stands in stark contrast to the findings which were made by the trial judge in the case at bar, findings that Caldwell, J.A. did not “propose to supplant”.¹⁰⁵

116. On the facts of the case, as it was in *Johannson*, it was possible for a trier of fact to disbelieve the accused and find that he had actual or imputed knowledge of the files being made available but that did not give the Court of Appeal the authority to intervene. Having heard the evidence, the trial judge did not reject the Appellant’s testimony or accept the Crown’s position that he was not credible. Wilful blindness requires a finding to the effect that the accused intended to cheat the administration of justice by deliberately remaining ignorant of the particular fact. Given the findings of the trial judge which were not overturned on appeal, it was not possible to come to a conclusion that the Appellant was wilfully blind.

117. Caldwell, J.A. reviewed the evidence which could have been used to find that the Appellant was wilfully blind.¹⁰⁶ It was open to the trial judge to reject the testimony of the Appellant and find he was not credible or that he was wilfully blind. However, the trial judge after considering the evidence reasonably came to the conclusion that he could not reject the Appellant’s evidence and that he was left with a reasonable doubt. Simply noting that there was evidence on which wilful blindness could have been found was not sufficient to set aside the acquittal and the Court of Appeal was in error in doing so.

PART IV – SUBMISSION AS TO COSTS

118. The Appellant makes no submission on the issue of costs.

¹⁰⁴ TJ, page 594

¹⁰⁵ CAJ, para. 91

¹⁰⁶ CAJ, para 88

PART V – ORDER REQUESTED

119. The Appellant requests the following relief:

- (a) That his appeal be granted on the issue of the reasonableness of the search for the IP address, that this Honourable Court rule that there was a breach of his section 8 *Charter* rights and that the evidence obtained in the search be excluded pursuant to section 24(2) of the *Charter*, the conviction quashed and an acquittal entered;
- (b) In the alternative, that the decision of the Saskatchewan Court of Appeal be set aside on the charge of making available child pornography contrary to section 163.1(2) of the *Criminal Code* and the trial judgment be restored dismissing the charge against the Appellant.

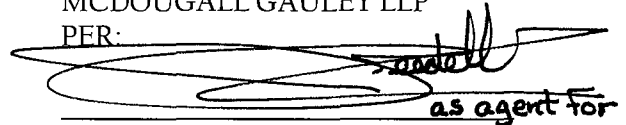
ALL OF WHICH IS RESPECTFULLY SUBMITTED.

Dated at the City of Regina, in the Province of Saskatchewan, this 15th day of May, A.D.

2013.

MCDUGALL GAULEY LLP

PER:

A handwritten signature in black ink, appearing to read "A. Fox", is written over a horizontal line. Below the line, the text "as agent for" is written in a cursive, handwritten style.

AARON A. FOX, Q.C. and
DARREN K. KRAUSHAAR
Counsel for the Appellant,
Matthew David Spencer

PART VI – TABLE OF AUTHORITIES

<u>Cases</u>	<u>At Para.</u>
<i>Dedman v. The Queen et al</i> , [1985] 2 SCR 2	80
<i>Hunter v. Southam Inc.</i> , [1984] 2 SCR 145	89
<i>Korponay v. Canada (Attorney General)</i> , [1982] 1 SCR 41	51
<i>R. v. Borden</i> , [1994] 3 SCR 145 at 162	51
<i>R. v. Briscoe</i> , 2010 SCC 13	109
<i>R. v. Buhay</i> , 2003 SCC 30	60
<i>R. v. Duarte</i> , [1990] 1 SCR 30	84
<i>R. v. Edwards</i> , [1996] 1 SCR 128	48, 58
<i>R. v. Gomboc</i> , [2010] 3 SCR 211	44, 64, 70
<i>R. v. Grant</i> , 2009 SCC 2	90
<i>R. v. Johansson</i> , 2008 SKQB 451 (Quicklaw)	114, 115, 116
<i>R. v. Jorgensen</i> , [1995] 4 S.C.R. 55	108, 109
<i>R. v. Kwok</i> , 2008 OJ No. 2414 (Quicklaw)	55
<i>R. v. Morelli</i> , 2010 SCC 8	22, 41, 90, 92, 94, 95
<i>R. v. Patrick</i> , 2009 SCC 17	49, 53
<i>R. v. Plant</i> , [1993] 3 SCR 281	46, 77
<i>R. v. Pugliese</i> , (1992) 71 CCC (3d) 295 Ont.CA. (Quicklaw)	58
<i>R. v. Rutten</i> , 2006 SKCA 17 (Quicklaw)	51
<i>R. v. Sansregret</i> , [1985] 1 S.C.R. 570	106, 107, 109
<i>R. v. Smith</i> , 2008 ONCA 101; [2008] O.J. No. 465 (Quicklaw)	110
<i>R. v. TELUS Communications Co.</i> , 2013 SCC 16	42
<i>R. v. Tessling</i> , (2004) 3 SCR 432	47
<i>R. v. Therens et al</i> , [1985] 1 SCR 613	80
<i>R. v. Trapp</i> , 2011 SKCA 143 (Quicklaw)	27, 46, 86, 88
<i>R. v. Ward</i> , 2012 ONCA 660 (Quicklaw)	56, 86

<i>R. v. Wong</i> , [1990] 3 SCR 36	85
<i>R. v. Woods</i> , 2004 MBCA 46 (Quicklaw)	80
<i>R. v. Woods</i> , [2005] 2 SCR 205	80
<i>Re S.C.</i> , 2006 ONCJ 343 (Quicklaw)	55

Texts

<i>Procedure in Canadian Criminal Law</i> , 2nd Edition (Toronto: Carswell, 2005)	79
---	----

PART VII – STATUTORY PROVISIONS

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11

Sections 8, 24(2)

Criminal Code of Canada (R.S.C.) 1985 Ch. C-46

Sections 163.1(2), 163.1(3), 163.1(4), 487 and 487.014(1)

Personal Information Protection and Electronic Documents Act, S.C. 2000, C-5

Section 7(3)(c.1)(ii)

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. Search or seizure

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

8. Fouilles, perquisitions ou saisies

Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

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

24(2) Exclusion of evidence bringing administration of justice into disrepute

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.

24(2) Irrecevabilité d'éléments de preuve qui risqueraient de déconsidérer l'administration de la justice

Lorsque, dans une instance visée au paragraphe (1), le tribunal a conclu que des éléments de preuve ont été obtenus dans des conditions qui portent atteinte aux droits ou libertés garantis par la présente charte, ces éléments de preuve sont écartés s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice.

Criminal Code

R.S.C., 1985, c. C-46, s. 163.1(2)

163.1(2) Making child pornography

Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of

- (a) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or
- (b) an offence punishable on summary conviction and is liable to imprisonment for a term not exceeding two years less a day and to a minimum punishment of imprisonment for a term of six months.

163.1(2) Production de pornographie juvénile

Quiconque produit, imprime ou publie, ou a en sa possession en vue de la publication, de la pornographie juvénile est coupable :

- a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an;
- b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois.

Criminal Code

R.S.C., 1985, c. C-46, s. 163.1(3)

163.1(3) Distribution, etc. of child pornography

Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or

(b) an offence punishable on summary conviction and is liable to imprisonment for a term not exceeding two years less a day and to a minimum punishment of imprisonment for a term of six months.

163.1(3) Distribution de pornographie juvénile

Quiconque transmet, rend accessible, distribue, vend, importe ou exporte de la pornographie juvénile ou en fait la publicité, ou en a en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité, est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de deux ans moins un jour, la peine minimale étant de six mois.

Criminal Code

R.S.C., 1985, c. C-46, s. 163.1(4)

163.1(4) Possession of child pornography

Every person who possesses any child pornography is guilty of

- (a) an indictable offence and is liable to imprisonment for a term of not more than five years and to a minimum punishment of imprisonment for a term of six months; or
- (b) an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.

163.1(4) Possession de pornographie juvénile

Quiconque a en sa possession de la pornographie juvénile est coupable :

- a) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans, la peine minimale étant de six mois;
- b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatre-vingt-dix jours.

Criminal Code

R.S.C., 1985, c. C-46, s. 487

487(1) Information for search warrant

A justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed,

(b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,

(c) anything that there are reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant, or

(c.1) any offence-related property,

may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(d) to search the building, receptacle or place for any such thing and to seize it, and

(e) subject to any other Act of Parliament, to, as soon as practicable, bring the thing seized before, or make a report in respect thereof to, the justice or some other justice for the same territorial division in accordance with section 489.1.

487(2) Endorsement of search warrant

If the building, receptacle or place is in another territorial division, the justice may issue the warrant with any modifications that the circumstances require, and it may be executed in the other territorial division after it has been endorsed, in Form 28, by a justice who has jurisdiction in that territorial division. The endorsement may be made on the original of the warrant or on a copy of the warrant transmitted by any means of telecommunication.

487(2.1) Operation of computer system and copying equipment

A person authorized under this section to search a computer system in a building or place for data may

(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

- (c) seize the print-out or other output for examination or copying; and
- (d) use or cause to be used any copying equipment at the place to make copies of the data.

487(2.2) Duty of person in possession or control

Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

- (a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;
- (b) to obtain a hard copy of the data and to seize it; and
- (c) to use or cause to be used any copying equipment at the place to make copies of the data.

487(3) Form

A search warrant issued under this section may be in the form set out as Form 5 in Part XXVIII, varied to suit the case.

487(4) Effect of endorsement

An endorsement that is made in accordance with subsection (2) is sufficient authority to the peace officers or public officers to whom the warrant was originally directed, and to all peace officers within the jurisdiction of the justice by whom it is endorsed, to execute the warrant and to deal with the things seized in accordance with section 489.1 or as otherwise provided by law.

487(1) Dénonciation pour mandat de perquisition

Un juge de paix qui est convaincu, à la suite d'une dénonciation faite sous serment selon la formule 1, qu'il existe des motifs raisonnables de croire que, dans un bâtiment, contenant ou lieu, se trouve, selon le cas :

- a) une chose à l'égard de laquelle une infraction à la présente loi, ou à toute autre loi fédérale, a été commise ou est présumée avoir été commise;
- b) une chose dont on a des motifs raisonnables de croire qu'elle fournira une preuve touchant la commission d'une infraction ou révélera l'endroit où se trouve la personne qui est présumée avoir commis une infraction à la présente loi, ou à toute autre loi fédérale;
- c) une chose dont on a des motifs raisonnables de croire qu'elle est destinée à servir aux fins de la perpétration d'une infraction contre la personne, pour laquelle un individu peut être arrêté sans mandat;
- c.1) un bien infractionnel,

peut à tout moment décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou

provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

d) d'une part, à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir;

e) d'autre part, sous réserve de toute autre loi fédérale, dans les plus brefs délais possible, à transporter la chose devant le juge de paix ou un autre juge de paix de la même circonscription territoriale ou en faire rapport, en conformité avec l'article 489.1.

487(2) Le mandat de perquisition doit être visé

Lorsque le bâtiment, contenant ou lieu est situé dans une autre circonscription territoriale, le juge de paix peut délivrer son mandat dans la même forme, modifiée selon les circonstances, et celui-ci peut être exécuté dans l'autre circonscription territoriale après avoir été visé, selon la formule 28, par un juge de paix ayant juridiction dans cette circonscription; le visa est apposé sur l'original du mandat ou sur une copie transmise à l'aide d'un moyen de télécommunication.

487(2.1) Usage d'un système informatique

La personne autorisée à perquisitionner des données contenues dans un ordinateur se trouvant dans un lieu ou un bâtiment peut :

a) utiliser ou faire utiliser tout ordinateur s'y trouvant pour vérifier les données que celui-ci contient ou auxquelles il donne accès;

b) reproduire ou faire reproduire des données sous forme d'imprimé ou toute autre forme intelligible;

c) saisir tout imprimé ou sortie de données pour examen ou reproduction;

d) utiliser ou faire utiliser le matériel s'y trouvant pour reproduire des données.

487(2.2) Obligation du responsable du lieu

Sur présentation du mandat, le responsable du lieu qui fait l'objet de la perquisition doit faire en sorte que la personne qui procède à celle-ci puisse procéder aux opérations mentionnées au paragraphe (2.1).

487(3) Formule

Un mandat de perquisition décerné en vertu du présent article peut être rédigé selon la formule 5 de la partie XXVIII, ajustée selon les circonstances.

487(4) Effet du visa

Le visa apposé conformément au paragraphe (2) constitue une autorisation suffisante pour que les agents de la paix ou fonctionnaires publics à qui le mandat a été d'abord adressé, et tous les agents de la paix qui ressortissent au juge de paix qui l'a visé, puissent exécuter le mandat et s'occuper des choses saisies en conformité avec l'article 489.1 ou d'une autre façon prévue par la loi.

Criminal Code

R.S.C., 1985, c. C-46, s. 487.014

487.014(1) Power of peace officer

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.

487.014(1) Pouvoir de l'agent de la paix

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.

***Personal Information Protection and
Electronic Documents Act***

s.c. 2000, C-5

7(3) Disclosure without knowledge or consent

For the purpose of clause 4.3 of Schedule I, 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

(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

(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

7(3) Communication à l'insu de l'intéressé et sans son consentement

Pour l'application de l'article 4.3 de l'annexe I 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 :

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 :

(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,