File Number: 34644

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

BETWEEN:

MATTHEW DAVID SPENCER

APPELLANT
(APPELLANT AND RESPONDENT IN THE COURT OF APPEAL)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(RESPONDENT AND APPELLANT IN THE COURT OF APPEAL)

FACTUM OF THE RESPONDENT
(Pursuant to Rule 42 of the *Rules of the Supreme Court of Canada*)

Anthony B. Gerein
Ministry of Justice
for the Province of Saskatchewan
Public Prosecutions
300 - 1874 Scarth Street
Regina, Saskatchewan S4P 4B3
Phone: (306) 787-5490
Fax: (306) 787-8878
Email: tony.gerein@gov.sk.ca
(Counsel for the Respondent)

Henry S. Brown, Q.C.
Gowling Lafleur Henderson LLP
Barristers and Solicitors
2600 - 160 Elgin Street
Ottawa, Ontario K1P 1C3
Phone: (613) 232-1781
Fax: (613) 563-9869
(Ottawa Agent for the Respondent)

McDougall Gauley LLP
Barristers and Solicitors
1500 - 1881 Scarth Street
Regina, Saskatchewan, S4P 4K9
Aaron A. Fox, Q.C. and Darren K. Kraushaar
(Counsel for the Appellant)
PHONE: (306) 757-1641
FAX: (306) 359-0785

McMillan LLP
Barristers and Solicitors
300 - 50 O'Connor Street
Ottawa, Ontario, K1P 6L2
Jeffrey W. Beedell
(Ottawa Agent for the Appellant)
PHONE: (613) 232-7171
FAX: (613) 231-3191

TABLE OF CONTENTS

PART I

CONCISE OVERVIEW OF THE RESPONDENT'S POSITION

1. The Appellant used a file sharing program to obtain child pornography from the computers of other people sharing files on the internet. He then left that child pornography in the part of his computer that would share it all with others whenever he was online.

2. And that is how the investigator found him. Actually, that is how the investigator found someone was sharing the files; identifying the Appellant took a little longer and a search warrant. First, the investigator asked the internet service provider for the name and address of the subscriber assigned the connection the pornography sharer used. The internet service provider chose to help.

3. It turned out that the internet connection belonged to the Appellant's sister. Only after the investigator learned her address, then obtained and executed the warrant, did he learn that the Appellant was living with her and using the internet connection for which she had subscribed.

4. The Appellant seeks to overturn his subsequent conviction for possessing child pornography, arguing that his privacy rights were infringed by the police asking for his sister's subscriber information even though the information was not his, it revealed nothing about his personal life, its disclosure was permitted (and anticipated) by the user agreement with the internet service provider and by statute, and even though the provider was legally entitled to decide whether to cooperate. He also argues that the trial judge rightly acquitted him of making child pornography available, even though the judge wrongly required an "active" effort to share files and consequently narrowed the intent for the offence. With respect, the Appellant errs twice.

5. There is no objective reason to think that an internet service provider must keep such basic information as an address and a name private, let alone shield it from a child pornography investigator. The Appellant's view would extend privacy to essentially all information, something inconsistent with the purpose and intent of s. 8 of the *Charter*. The Court of Appeal was right to find against him. Similarly, and as the Appellant concedes that the crime of making child pornography available does not require an active step, the Court of Appeal was right to say the trial judge erred as to intent in a way that needs correcting.

THE FACTS

The Charges and The Images

6. The Appellant's summary of the facts is incomplete, so a fuller review is required. As this Court knows, the Appellant went to trial charged that, between August 31, 2007, and September 20, 2007, at or near Saskatoon, Saskatchewan, he 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; and
>
> make available child pornography, when 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(3) of the Criminal Code.
>
> *Indictment, Appellant's Record, page 87*

7. The still images and videos tendered by the Crown, and which the Appellant acknowledged to be child pornography, were vile:

> [They] included the display of infant genitalia, the manipulation by adults and infant boys attempting vaginal intercourse with an adult female. These were more than sufficient to convince any reasonable observer that what the images were portraying were disgusting, demeaning, depraved activities of child abuse of the worst order.
>
> *Queen's Bench Reasons for Judgment, Appellant's Record, page 16 (590), lines 18 - 25*

The Crimes and the Investigation

8. Between August 31, 2007, and September 20, 2007, and for a long time before that, the Appellant frequently used a computer program called LimeWire to search for and download child pornography from other internet users who were then online and using the same or similar software. The child pornography downloaded into the Appellant's computer's "shared folder".

> *Queen's Bench Reasons for Judgment, Appellant's Record, page 15 (589), lines 14 - 22; Trial Transcript ("Transcript"), Testimony of Sergeant Parisien, Respondent's Record, page 6, line 2, through page 9, line 14; page 21, lines 1 through 3; Transcript, Testimony of the Appellant, Respondent's Record, page 43, lines 4 - 8; page 44, line 14 - page 45, line ;1 page 47, lines 17 - 20; Warned Statement Transcript, Respondent's Record, page 106*

9. LimeWire works by searching all such shared folders of all the computers connected to the internet at the time of the search which are running the same or similar file sharing software. However, LimeWire searches only the shared folder of each of those computers - it is the only portion open to file sharers - for material corresponding to the user's search request. It cannot search any other portion of someone else's computer.

Queen's Bench Reasons for Judgment, Appellant's Record, page 15 (589), line 23 - page 16 (590), line 11; page 17 (591), lines 8 - 19; Transcript, Testimony of Det. Sgt. Darren Parisien; Respondent's Record, page 4, line 10 - page 200, line 26

10. Just as the Appellant was able to use the software to search the shared folder of other computer users while online, their software was able to search his. It was in this way that Detective Sergeant Parisien, an investigator with the Saskatoon Police Services assigned to the Saskatchewan Internet Child Exploitation Unit and before that doing the same work with the Vice Unit, discovered the child pornography. Using similar, publicly available software, he simply searched for anyone sharing child pornography. His software found it in the shared folder of the Appellant's computer, and in the shared folders of many others.

Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 2, line 10 - page 3, line 1; page 5, lines 6 - 24; 22, line 18 - page 23, line 2; page 20, lines 13 through 24; at the time Sgt. Parisien was on line, the Appellant was sharing 186 files - page 23, lines 17 through 27; later in the investigation, he was sharing 441 files - page 25, line 4 through page 26, line 16

11. To be absolutely clear, as the Appellant was using LimeWire file sharing software, the only thing Det. Sgt. Parisien could access in the Appellant's computer was whatever the Appellant had in his shared folder, the folder open to the public. The Appellant's suggestions to the contrary are unsupported and incorrect.

Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 7, line 13 - page 9, line 14; page 10, lines 3 - 26

12. The officer could not tell whose computer was involved, where it was, or anything about the user. All he could determine were two numbers. The first was the Internet Protocol address" ("IP address"), which corresponds to the particular internet connection through which a computer links

to the net at that time [one might say it is akin to a telephone number, or an entrance ramp onto the "information superhighway"].

> *Preliminary Hearing Transcript ("PHT"), Respondent's Record, page 63 lines 1 - 12; page 64, line 16 - page 65, line 4* (The Charter challenge took place at the outset of the trial, on the strength of the Preliminary Hearing transcript. The Appellant did not testify on the Charter application.)

13. The IP address is not secret; the IP address of the computer from whom one obtains shared material is actually offered up by that computer, displayed as part of the file sharing process. The IP address does not facilitate access to anything more than what a person chooses to share. Contrary to the Appellant's assertion, and on the evidence, it does not open a window on one's internet habits.

> *Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 11, line 3 - page 13, line 14; PHT, Respondent's Record, pages, 64, 65, and page 69, question and answer 20*

14. Using publicly available software and police databases, the officer was able to determine the rough geographical location of the IP address used by each computer that had shared child pornography with him at the time of his search. Amongst those, he identified a connection in Saskatoon, Saskatchewan, a connection owned by Shaw Communications ("Shaw").

> *PHT, Respondent's Record, pages 67 and 76; page 80, lines 25 - 26; Trial Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 18, line 11 -page 19, line 11*

15. The investigator made a written request of Shaw for information respecting the customer holding the particular IP address at the specific time he discovered the shared child pornography. He sought the customer name, the street address where the internet connection was actually located, the current service status, and the telephone number tied to it, pursuant to s. 7(3) of the *Personal Information Protection and Electronic Documents Act* (*"PIPEDA"*).

> *PHT., Respondent's Record, pages 81 - 82; page 963; Trial Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 27, line 21, through page 28, line 25; Information Request, Appellant's Record, pages 123-125*

16. Shaw's policies, as posted on the Shaw website, permitted the company to respond to *PIPEDA* requests. Those policies advise that Shaw may disclose customer information to an

investigator in certain circumstances. Though the officer could not say if such policies had actually been provided to the Appellant or his sister by Shaw, he could say that the policies are found online at Shaw's website, and insofar as they relate to matters such as child pornography the policies have remained of the same substance for many years.

PHT, Respondent's Record, pages 88 - 92, 97 - 99

17. Shaw replied, sending information identifying the Appellant's sister - she was the sole party to the internet service contract - and giving her address. The investigator then did up a search warrant application for the apartment at the address provided.

PHT, Respondent's Record, pages 78 and 85; Shaw Response, Appellant's Record, pages 126 - 127

18. After obtaining a search warrant and searching the residence, the police learned the Appellant lived with his sister and that he was the one who had shared the child pornography. Until searching the house, Det. Sgt. Parisien "didn't even know he existed".

Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 29, line 2, through page 31, line 26; page 32, lines 6 through 10

19. The second number file sharing provides is called a GUID number. LimeWire and similar software assigns a unique number to each computer using it. The police used the GUID number to confirm the exact computer involved in the crimes here.

PHT, Respondent's Record, pages 78 and 85; Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page 13, line 15 - 17, line 8

20. The Crown stresses that until the execution of the search warrant the police were never able to see anything more of the Appellant's internet activities than what the Appellant chose to make available through the shared folder. Neither Detective Parisien nor anyone else had access to the Appellant's e-mails, texts, or any part of his computer.

PHT,Respondent's Record, pages 69 and 100 - 101

Possession of Child Pornography

21. The Appellant had copious quantities of child pornography in his shared folder. At one point the total was 441 still images and 112 videos. He admitted searching it out. His argument turned only on whether the police needed a warrant to obtain his sister's subscriber information.

Queen's Bench Reasons for Judgment, Appellant's Record, page 18 (592), lines 12 - 16

Making Child Pornography Available

22. At trial, the Appellant testified that he did not know that LimeWire worked through a file sharing methodology, rather than drawing material from a central computer server, until he was questioned by Det. Sgt. Parisien. Indeed, he claimed ignorance of the fact his shared folder was open to others. That was after the search of his residence and seizure of his computer.

Queen's Bench Reasons for Judgment, Appellant's Record, page 19 (593), lines 2 - 21; Transcript, Testimony of the Appellant, Respondent's Record, page 46, line 20 - page 47, line 16

23. The Crown argued the Appellant's intent could and should be inferred from various things:

LimeWire is and holds itself out to be a file sharing program, not an internet search engine;

When setting up LimeWire, the screens contain information notifying the user that it is a file sharing program;

Indicators that LimeWire is a file sharing program come up on the screen as part of, and in the course of, using it, along with warnings about the ramifications;

The top of each screen talks about information sharing when using LimeWire;

There are indications shown on the screen when someone copies files from the user's shared folder;

The Appellant had used LimeWire for many years;

The default share function was not turned off, but could have been; and

Another setting on the Appellant's computer was changed from the default setting, the setting for the maximum number of files which could be downloaded was increased.

Queen's Bench Reasons for Judgment, Appellant's Record, page 19 (593), line 22 - page 20 (594), line 12; Trial Transcript, Testimony of Det. Sgt. Parisien, Respondent's Record, page

24, lines 21 - 26; page 337, lines 3 - 11; page 33, line 26 - 37, line 18; page 48, lines 6 - 13; page 38, lines 10 - 17; pages 39, line 3 - page 42, line 6

24. Then there was this warned admission from the Appellant:

> S I don't even know how it works. Like it, trying to think like it's file share, eh, so I mean it must, ha, I don't know like I know people have said you shouldn't use Limewire because, people, can access it and stuff but like, I don't really understand that, that (inaudible).
>
> P Um hmm, you understand its file sharing, right?
>
> S Yup
>
> P So that means to you what is filing (sp) sharing mean?
>
> S I guess I can get your files and you can get mine.
>
> *Warned Statement Transcript, Respondent's Record, page 104, line 20 - page 105, line 4*

25. The Appellant confirmed his understanding that, to him, "shared folder" means "everyone can have it" (lines 20 - 22). He later claimed that he realized this thanks to Sgt. Parisien's questioning, but note this admission:

> P I mean I never even thought that's a bogus answer. You never thought about that (sic) the fact that you're on a file sharing program, that you're sharing files? You got to be kidding me?
>
> S Well, I knew I was, like I guess I just never, I just (inaudible)
>
> P I'll maybe put it to you this way, you didn't really care. OK, cause there's no way you didn't know it was happening. There's no way you, there's nothing you did to stop it from happening, you could have disconnected, you could have shut down all of your Limewire and just gone with what you had, but, the real answer is you didn't care.
>
> S Which is just sick, but it's true.
>
> *Ibid., page 107, lines 11 - 20; Transcript, Testimony of the Appellant, Respondent's Record, page 49, lines 12 -23; page 50, lines 2 - 24; and page 51, line 9 - 52, line 6*

The Trial Judge's Conclusions - Guilty of Possession but not of Making Available

26. The learned trial judge found no reasonable expectation of privacy in regards to the subscriber information, and thus no s. 8 *Charter* violation. The learned trial judge convicted the Appellant of possession of child pornography,

Voir Dire Reasons, Appellant's Record, pages 8-9, pars. 17 - 19

27. The judge then concluded that the Appellant did not knowingly share the files he possessed through LimeWire, so the judge acquitted him of the making available charge:

> In this case Mr. Spencer did not take active facilitation steps that would serve as an indicator of intent. 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.
>
> From this I think it is very difficult to conclude that he had the knowing, live intention to distribute or make child pornography available to others.... There is, in my view, a reasonable doubt. I therefore find him not guilty of count 2.
>
> *Queen's Bench Reasons for Judgment, Appellant's Record, page 25 (599), line 6 - 22*

The Court of Appeal: Guilty of Possession and a New Trial on Making Available

28. The Appellant appealed his conviction for possession of child pornography, arguing that the trial judge erred by finding no s. 8 violation respecting the subscriber information from Shaw. The Crown appealed the acquittal on the making available charge, submitting that the trial judge wrongly required a 'positive step' by the Appellant before he would find the necessary criminal intent.

29. As regards the search and seizure argument, Caldwell, J.A. found that no search took place. Following the steps set down by this Court, he concluded that while the Appellant had a subjective expectation of privacy in the subscriber information, there was no objectively reasonable expectation. Though Caldwell, J.A., considered the information to be within "the biographical core of personal information... information tending to reveal intimate details of the lifestyle and personal choices of the individual" as it "did ultimately reveal intimate details of lifestyle and personal choices of Mr. Spencer, and his activities within his home", the terms of the service agreement documents should be read to apply to any user of the internet connection, and those terms allowed Shaw to cooperate with law enforcement, removing any reasonable expectation of privacy. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA)* allows for such agreement.

> *Court of Appeal Reasons, Appellant's Record starting at page 28, , pars. 17, 20, 22, 27, 32 and 33, 38, 39 - 45*

30. Had Caldwell, J.A., found a reasonable expectation of privacy, he nonetheless would have held the search lawful under s. 487.104 of the *Criminal Code* and reasonable.

Ibid., par. 46

31. For his part, Cameron, J.A., expressed reservations about whether the contractual arrangement with Shaw and the other circumstances outweighed what he saw as core biographical information, but still concurred in the result. To him, the search was reasonable under s. 487.014.

Ibid., pars. 96 - 99

32. Ottenbreit, J.A., also concurred in the result, though he arrived at it by a different course; for him, the information sought was in no way core biographical data engendering a reasonable expectation of privacy. No matter the potential for the information to lead to disclosure of the Appellant's personal activities, it actually revealed nothing about such things:

> Theoretically, all the assertions in an information to obtain a search warrant have the potential of revealing to the police more intimate details of a person once the search warrant is granted and executed. In this respect the Disclosed Information has, in my view, no different special quality than any other piece of information that the police may receive prior to the warrant which furthers their investigation.
>
> *Ibid., par. 110*

33. Caldwell, J.A., thought the acquittal on the make available charge should be overturned and a new trial ordered. He rejected the trial judge's view that conviction required a positive step; the trial judge erred in equating "making available" with offences such as "distribution".

Ibid., pars. 69, 70, 72, 77, 78, and 79

34. That meant even though the trial judge found the Appellant did not "know" he was making child pornography available, the trial judge failed to consider wilful blindness. Since there was "considerable evidence to the effect that Mr. Spencer might have had an actual suspicion that his file sharing program (LimeWire) shared his files with others", there must be a new trial. Ottenbreit, J.A., and Cameron, J.A. concurred.

Ibid., par 87, 88 - 95, par. 100 - 106

PART II

QUESTIONS IN ISSUE

35. With respect, the issues need to be stated more precisely than the Appellant has done.

36. Was there a reasonable expectation of privacy in the subscriber information? No.

37. If so, was the police search unreasonable? No.

38. If this Court finds a breach of s. 8, should the evidence linking the Appellant to the child pornography be excluded under s. 24(2)? No.

39. Was the Court of Appeal correct in finding the trial judge required more than passive sharing to make out the intent component of the making available offence? Yes.

40. If the judge did require more than passive sharing, did he err as to the necessary intent? Yes.

PART III

ARGUMENT

Access to, the possession of, and trafficking in child pornography over the Internet present serious and pressing societal problems. Easy entry to the Internet, from almost anywhere, the international nature of the trade in child pornography, and user anonymity combine to make effective law enforcement difficult.

R. v. Ward (2012), 112 O.R. (3d) 321 (Ont. C.A.), at par. 1

I. There is No Reasonable Expectation of Privacy in a Name and Street Address

A. Overview - The Appellant Would Take Privacy Too Far

41. This part of the appeal presents a narrow issue: does a person enjoy a reasonable expectation of privacy in subscriber information? Put another way, should the police have to get judicial authorization to determine the physical address of an internet connection and the subscriber's name before they apply for judicial authorization to search that physical address?

42. The answer to those questions must be "no", for the subscriber information sought says nothing more than that a particular person or company has an internet link. It says nothing about anyone who uses that link. The Appellant asserts that subscriber information reveals deeply private and personal things. He asserts that IP addresses are, in effect, a window on the internet life of a person. Both assertions are incorrect.

43. One has to look at the information actually in issue - the name and address of the subscriber - not the child pornography the Appellant had already made available over the internet. To the extent the subscriber information allows for hypotheses about the person named and the place identified, that is not because of any quality within the subscriber information, but because of other facts the police have already, legally, acquired. To take up the Appellant's position would undermine decisions of this Court, including those in *R. v. Plant* and *R. v. Tessling*, where the whole of what the police gathered allowed for theories but the information actually in issue said little.

44. And yet the information in those cases revealed more than the subscriber information here. Names and addresses are largely innocuous, known to most everyone with whom we deal in society. They are in the telephone directory. The licensors of our vehicles, our employers, and the schools we attend know them. Our neighbours know us.

45. To find a reasonable expectation of privacy in such information simply because it has the potential, when combined with other information, to reveal deeper truths about us, would cloak essentially everything in privacy. Search warrants would be required for most every police inquiry and other citizens and corporate citizens would be improperly constrained from helping with law enforcement. That is neither true to the 'balancing' which underlies s. 8, nor workable.

B. The Onus was on the Appellant

46. The person alleging a violation of s. 8 of the *Charter* must establish that a reasonable expectation of privacy existed to obtain s. 8 protection.

R. v. Gomboc, [2010] 3 S.C.R. 211, par. 21

C. There is No Reasonable Expectation of Privacy in Subscriber Information

47. To go back to first principles, section 8 of the *Charter* guarantees to everyone "the right to be secure against unreasonable search or seizure". This constitutional guarantee is intended to protect people and not places, and it protects only to a reasonable extent.

Hunter v. Southam Inc., [1988] 2 S.C.R. 145, pp. 159-160, Appellant's Authorities, Tab 8; *R. v. Gomboc, supra*, par. 17

48. Privacy is the dominant organizing principle under section 8 of the *Charter*, and the expectation of privacy "is a normative rather than a descriptive standard". It takes three forms: (1) personal privacy; (2) territorial privacy, and (3) informational privacy.

R. v. Tessling, [2004] 3 S.C.R. 432, pars. 25 and 42

49. The Respondent submits that the Appellant is asserting informational privacy here. While there is geographical information involved, the privacy claim pertains to the subscriber information.

50. In *R. v. Tessling*, Justice Binnie, writing for a unanimous court, described informational privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others". He acknowledged that because privacy generally, and informational privacy particularly, is "a protean concept", it can be difficult to draw the line between reasonable and unreasonable.

Tessling, supra, pars. 23 and 25

51. To help alleviate some of the difficulty, he pointed to Justice Sopinka's majority opinion in *R. v. Plant.* Informational privacy means "a biographical core of personal information" including "information which tends to reveal intimate details of lifestyle and personal choices of the individual". Justice Binnie acknowledged that Justice Sopinka's descriptor of what qualified as a biographical core of personal information was not meant "to be exhaustive"; however, and key to this appeal, he emphasized that "*Plant* clearly establishes that not all information an individual may wish to keep confidential necessarily enjoys s. 8 protection".

Tessling, supra, par. 25; *R. v. Plant*, [1993] 3 S.C.R. 281, page 293

52. Notably, *Plant* saw this Court find no reasonable expectation of privacy in computerized electricity records. True, the records revealed "the pattern of electricity consumption in the residence [, but] cannot be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence".

Plant, supra, at pages 293 (quote) and 295-296

53. This Court, in *Tessling*, applied that approach to the question of whether a fly-over measurement of heat emissions from a home was a search. This Court found no reasonable expectation of privacy in such emissions, and so, no search.

R. v. Tessling, supra

54. Building on those cases, as well as *R. v. Edwards*, this Court refined the rubric in *R. v. Patrick.* On behalf of the majority, Justice Binnie enumerated the following considerations for assessing a privacy claim:

the nature or subject matter of the alleged search;

whether the section 8 claimant had a direct interest in the subject matter;

whether the section 8 claimant had a *subjective* expectation of privacy in the information contained in this subject matter; and

if so, whether the expectation was *objectively* reasonable.

Patrick, [2009] 1 S.C.R. 579, at par. 27; see also *Plant, supra*, at pp. 292-293, par. 26; *R. v. Edwards*, [1996] 1 S.C.R. 128, at pp. 145-146, Appellants Authorities, Tab 8

55. Several factors bear on objective reasonableness:

the place where the alleged search occurred;

whether the informational content of the subject matter was in plain view;

whether such information was already in the hands of third parties and, if so, was it subject to an obligation of confidentiality;

whether the police technique was intrusive in relation to the privacy interest;

whether the evidence-gathering technique was itself objectively unreasonable;

whether the informational content exposes intimate details of the section 8 claimant's lifestyle, or information of a biographic nature; and

if the analysis respecting the reasonable expectation of privacy is answered in the affirmative, was the reasonable expectation of privacy in the information violated by the police conduct?

Patrick, pars. 27 and 28

56. Using that approach here discredits the privacy claim respecting subscriber information.

(a) The Nature or Subject Matter of the Search Left No Reasonable Expectation of Privacy

57. The subject matter in issue is the information Shaw provided to the City of Saskatoon Police Service: the Appellant's sister's name and street address essentially. It was the address that mattered most. Unlike some case this Court has decided, computer privacy is not in issue.

58. Equally, and contrary to suggestions in the Appellant's factum, the IP address is not in issue, either. That address was volunteered by the Appellant's computer to the child pornography investigator's computer. And it did not enable the police to learn anything other than the general location of the computer and the identity of the Internet Service Provider ("ISP").

59. Finally, one must not lose sight of the fact that this is about the subscriber information alone, not what it reveals or potentially could reveal in conjunction with other things. On the evidence, the police could go no further than anyone else using file sharing software - looking only at what the Appellant chose to leave in his shared folder. There is no indication in the subscriber information as to who actually used the connection, what it was used for, or the Appellant's activities.

60. This Court, in *Plant*, made the same point when it held that a police check of computerized power consumption records, records in the possession of a public electrical utility but linked to the police station by a password, did not constitute a search. Justice Sopinka, writing for the majority, focussed only on the records when addressing the question of what they tended to reveal:

> "The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence."
>
> *Plant, supra,* page 293.

61. So, the Appellant's argument begins with a mistaken conjunction: he asks this Court to consider not just the subscriber information but to join it with the child pornography the police had already found. That is not the law. Nor should it be, for whether or not there is a search must focus on the information sought/obtained. Next, he argues that the subscriber information reveals or potentially reveals intimate details about anyone living at the civic address, so privacy goes that far. That was not the evidence. Really, this is simply about an address and a name.

(b) The Appellant Had No Interest in the Subject Matter

62. In *Patrick*, Justice Binnie recalls that at this stage of the analysis the "issue is not whether the appellant has a legitimate privacy interest" in the information, but rather "whether people generally have a privacy interest" in such information.

> *Patrick, supra*, at par. 32

63. People who share a residence with others have a privacy interest in the premises, and the activities undertaken there, but do not and ought not to be taken to have a privacy interest in the name and address other residents provide to companies pursuant to contracts (telephone service,

television service, internet connection, and so on). While at least one case - *R. v. Vasic* - has held otherwise, the Crown submits that it conflates privacy in the use of the service with privacy respecting the contract itself. A person has no privacy interest in another's 'tombstone data'. That comes clear upon considering *R. v. Pervez*, where one of the reasons the Alberta Court of Appeal found no reasonable expectation of privacy in the accused's sister's cell phone records was because he did not control the information:

> One measure of an individual's privacy interest is whether that the person can assert any control over the records. Pervez was not able to do so. If, for example, he had contacted the service provider to demand copies of the records, the provider could have refused and Pervez would have had no recourse. It is doubtful that Pervez even knew of the existence of some of the information. It was created for legitimate commercial purposes. It was subject to a commercial contract, to which Pervez was not a party.
>
> Persons who want to maintain privacy rights have, at a minimum, to structure their affairs in a manner consistent with that desire. Using a cell phone that is owned by another party does not entitle the user to a privacy interest over records that are relevant to the relationship between the cell phone provider and the owner of the cell phone.
>
> *R. v. Pervez* (2005), 367 A.R. 165 (Alta. C.A.), pars. 13 and 14; *R. v. Vasic* (2009), 2009 CanLii 6842 (Ont. S.C.) at pars 43 through 48

(c) The Appellant Had No Subjective Expectation of Privacy

64. The trial judge found no subjective expectation of privacy, as pointed out by the Crown when in the Court of Appeal. Based on the evidence that was a reasonable finding of fact and the Court of Appeal erred in presuming otherwise.

Voir Dire Reasons, Appellant's Record, pages 3 and 9, pars. 2 and 18

65. The Court of Appeal's contrary presumption appears to have come from a focus on the fact the Appellant used a computer in his home. As stated, that was not and is not relevant.

Court of Appeal Reasons, Appellant's Record, pages 34 and 35, par. 17

66. There was no direct evidence from the Appellant that he had a subjective expectation of privacy in the information provided by Shaw. He did not testify on the s. 8 voir dire at the outset of

the trial. Later, testifying after the Crown closed its case, he did not give evidence on the point. While in *Patrick* the absence of direct evidence from the accused about his subjective expectation of privacy did not defeat such a claim, and while this stage of the analysis does not present "a high hurdle", that stemmed in part from this Court's view that "in the case of information about activities taking place in the home, such an expectation is presumed in the [accused's] favour". Here, as argued above and, further, below, the subscriber information does not illuminate activities within the home or anything about the Appellant. Coupling those facts with the fact that the name and address of the subscriber related to and were given by another person - his sister - to a private business as part of a contract which included the prospect of that business monitoring use of the connection and disclosing to the police upon request or in other circumstances (as set out shortly), leaves no room for an inference of a subjective expectation of privacy.

Voir Dire Reasons, Appellant's Record, page 3, par. 2; Patrick, supra, at par. 37

(d) There is no Objectively Reasonable Expectation of Privacy in Subscriber Information

67. The Respondent submits that even if there was a subjective expectation of privacy in the information disclosed by Shaw to Detective Sergeant Parisien, there is no objectively reasonable expectation of privacy in circumstances like these. The objective factors enumerated in *Patrick* lead to that conclusion, always remembering that this is not about an internet user's expectation of privacy writ large, as the Appellant suggests, but about a third party's claim to privacy in someone else's name and address *vis-a-vis* a child pornography investigation.

(i) The Place Where the Alleged Search Occurred Left no Expectation of Privacy

68. The search took place somewhere in the corporate offices of Shaw, a place in which the Appellant had no reason to expect privacy. It compares to the accused's girlfriend's apartment in *R. v. Edwards,* where the accused had no reasonable expectation of privacy either.

R. v. Edwards, supra, Appellant's Authorities, Tab 8

69. In *Plant*, the electricity records had been generated by a third party, the City of Calgary's electrical utility. In *Tessling*, the degree of heat emanating from a private residence could not be

controlled. In *R. v. M.(A.)*, this Court explained that the holdings in both *Plant* and *Tessling* "were premised on the finding that the information had already escaped the possession and control of the suspect". Here, the Appellant's sister surrendered control over her information to Shaw at Shaw's location. How could the Appellant have any expectation regarding it?

> *R. v. M.(A.)*, 2008 SCC 19, at par. 19; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393 - where a student had a higher expectation of privacy as to his person than as to the school environment.

(ii) The Information Was not in Public View

70. The subscriber information was not on public view; however, names and addresses are available in a city telephone directory and city records. Neighbours know who lives in their neighbourhood. It is also information commonly found with ease.

(iii) The Third Party Had the Information Subject Only to Limited Confidentiality

71. The obligations a Shaw customer assumes upon contracting with the corporation are available on the company's website, as testified to by Sgt. Parisien. He was not contradicted. The "Joint Terms of Service" document makes it plain that Shaw may disclose information as it thinks it necessary. Compellingly, that comes under the heading "Confidentiality":

> Confidentiality
>
> Shaw may disclose any information as is necessary to:
>
> a. Satisfy any legal, regulatory or other government request;
>
> b. Operate the Services properly;
>
> c. Or protect Shaw or its customers, in accordance with the guidelines set out in Shaw's Privacy Policy.
>
> *Shaw Joint Terms of Service Policy, Appellant's Record, page 143*

72. Section 3.3. of Shaw's Privacy Policy allows for disclosure without consent, "as permitted by law".

> *Shaw Privacy Policy, Appellant's Record, page 131*

73. Section 3.4 of the same policy permits Shaw to disclose where required by law and in accordance with PIPEDA. Shaw "may disclose Customer's Personal Information" to:

> f. A third party or parties, where the Customer has given Shaw Consent [sic] to such disclosure or if disclosure is required by law, in accordance with *The Personal Information Protection and Electronic Documents Act.*
>
> *Ibid., page 132*

74. Shaw's Acceptable Use Policy expressly states, on its second page, that dealing with child pornography violates the contract and the subscriber is responsible even for the misuse of the internet account by others. Soon after, under the heading "Inappropriate Content", it indicates that Shaw may monitor content and has the right to disclose illegal activity in accordance with the Privacy Policy:

> Shaw has no obligation to monitor transmissions made on the Services. However, Shaw has the right to monitor such transmissions and to disclose the same in accordance with Shaw's Privacy Policy.
>
> *Shaw's Acceptable Use Policy, Appellant's Record ,page 146*

75. The seventh page of the Acceptable Use Policy is the key; it authorizes Shaw to cooperate unilaterally with law enforcement officers:

> You hereby authorize Shaw to cooperate with (i) law enforcement authorities in the investigation of suspected criminal violations, and/or (ii) system administrators at other Internet service providers or other network or computing facilities in order to enforce this Agreement. Such cooperation may include Shaw providing the username, IP address, or other identifying information about a subscriber, in accordance with the guidelines set out in Shaw's Privacy Policy.
>
> *Ibid., page 150*

76. Such express authorization to cooperate with the child exploitation investigator here, alone and combined with the other contractual terms, would leave a reasonable person understanding that Shaw will not condone the use of its internet connections for illegal activities, in particular activities involving child pornography. In the event of such an abuse, a reasonable person would expect Shaw to cooperate with the police. That is part of the bargain - a company need not give impunity along with internet access, and there is nothing wrong with a person trading a certain amount of privacy for access.

77. While the Appellant suggests it was never proven he read or agreed to the terms of the contract, that is irrelevant to this part of the analysis. A reasonable person would be taken to have read it, especially if the matter of privacy on the internet is as important as the Appellant claims.

78. Contracts are relevant to expectations; so are statutes. In *Gomboc*, police had suspicions a house was being used for a marijuana grow operation. They asked the electrical company, Enmax, to place a digital Recording Ammeter on the powerline to the house so they could determine whether the timing and pattern of electrical usage was consistent with such an operation. The company did so. The majority found great significance in the applicable *Code of Conduct Regulation,* which allowed disclosure of information to the police unless contrary to the express request of the customer. Mr. Gomboc had not made such a request. For the majority, that dovetailed with s. 487.014 of the *Criminal Code*, which allows a peace officer to ask a person to voluntarily provide information if there is no lawful impediment to their providing it. Any expectation of privacy falls. So too here.

Gomboc, supra, at pars. 31 through 33 as well as 55 through 58

79. Subsection 7(3) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) permits disclosing personal information for prescribed law enforcement purposes:

> 7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> ...
>
> (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
>
> (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
>
> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

...

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

(i) required by law.

80. Clause 4.3 of Schedule 1 reads:

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

81. The purpose of *PIPEDA* is set out in s. 3 of the Act, which seeks to balance privacy and openness for reasonable purposes:

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.

82. The Act applies to Shaw.

PIPEDA, s. 4(1) and s. 2

83. The Crown underscores that the language of subsection 7(3) of *PIPEDA* is permissive, not mandatory. As under the service contract, Shaw was at liberty to cooperate.

R. v. Wilson, [2009] O.J. No. 1067 (S.C.J.) at par. 39

84. The contract and *PIPEDA* leave no objectively reasonable expectation of confidentiality in the subscriber information. More so when combined with the other facts and considerations here.

R. v. Chehil, 2009 NSCA 111, at pars. 44-46

85. While *R. v. Gomboc* provides a compelling analogy here, and calls for the conclusion that the contractual relationship left no room for a reasonable expectation of privacy, the Ontario Court of Appeal's decision in *R. v. Ward* makes the point directly. It holds that service agreements, *PIPEDA*, and s. 487.014 of the *Criminal Code* bear on privacy expectations.

R. v. Ward (2012), 112 O.R. (3d) 321 (Ont. C.A.) pars. 41 - 50, 52 - 58, 105

86. Mr. Justice Doherty found *PIPEDA* and the contract terms (akin to those here) left no reasonable expectation of privacy in the face of a child pornography investigation and request:

> The contractual provisions in this case tend to reinforce my reliance on *PIPEDA* as indicative of the nature of the appellant's reasonable expectation of privacy. Like *PIPEDA*, the contractual terms speak both of Bell Sympatico's duty to protect the privacy of clients' information and its willingness to disclose information in relation to investigations involving the alleged criminal misuse of its services. That willingness clearly qualifies any duty of confidentiality assumed by Bell Sympatico. While there is no single provision in the agreement or related documents that spells out Bell Sympatico's willingness to disclose information to the police as clearly as did the regulation under consideration in *Gomboc*, the overall thrust of the documentation is to the same effect. In particular, the Accepted Use Policy ("AUP") makes it clear that uploading or downloading child pornography is a breach of the AUP and that Bell Sympatico would "offer full cooperation with law enforcement agencies in connection with any investigation arising from a breach of this AUP." That cooperation would, it seems to me, obviously extend to the disclosure of subscriber information which, by the terms of the service agreement, could be disclosed if "[n]ecessary to satisfy any laws, regulations or other governmental request ... or as necessary ... to protect ... others."
>
> *Ibid.*, at par. 100; See also *R. v. Cuttell* (2012), 296 O.A.C. 324 (Ont. C.A.) at par. 6

87. That was especially so when one looks at the limited picture the subscriber information provided would give the police as to Mr. Ward's activities. The same is true here.

Ibid., pars. 109

88. A final consideration is that reasonable privacy is not a guarantee of anonymity. Shaw, like the electrical company - Enmax - in *Gomboc* and the ISP in *Ward*), "had a legitimate interest of its own in the quantity of electricity its customers consumed". Enmax could have placed the DRA on its own and could have reported what it found to the police. The ISP in *Ward*, and Shaw in this case, could have done their own investigations and reported what they found to the police.

> ... Enmax was not an interloper exploiting its access to private information to circumvent the *Charter* at the behest of the state. As the Crown stresses in its submissions, Enmax's role is limited to the wholly voluntary cooperation of a potential crime victim. The coercive undertones evoked by describing Enmax as being co-opted or conscripted are entirely inapposite to the case at bar. As noted above, if the police had merely notified Enmax of a potential electricity theft and the utility had proceeded on its own initiative to install a DRA and turn over what it disclosed, no *Charter* violation would have arisen. Only by misguidedly elevating form over substance would a contrary conclusion result solely because Enmax installed the DRA subsequent to a police request for cooperation. Indeed, as mentioned, it is clear from s. 487.014 of the *Criminal Code* that no prior judicial authorization is necessary to cooperate with an investigation provided disclosure of the information requested is not otherwise prohibited by law."
>
> *Gomboc, supra*, pars. 41 through 43 (quote from par. 42); *Ward, supra*, par. 98; *R. v. Thomas* (2013), 2013 ABQB 223, at pars. 22 through 29

(iv) The Police Search Technique was not Intrusive

89. The following words from *Plant* apply just as well here:

> Accessing the information did not involve intrusion into places ordinarily considered private. Nor did it involve invasion by state agents in personal computer records confidentially maintained by a private citizen.
>
> *Plant, supra*, at p. 295

(v) The Evidence Gathering Technique was not Objectively Unreasonable

90. The question is whether using a request, authorized under section 7(3) of *PIPEDA,* undermines privacy with "the potential to make social life in this country intolerable". It does not.

Patrick, supra, at par. 70

91. The Saskatoon Police Service did not have unlimited or continuous access to the information in Shaw's database. The letter asked for information from just one moment in time, information which gave an address and a name, but no insight into the Appellant's internet activities. The subscriber information was useless without a subsequent warrant. That is not intolerable.

(vi) The Information does not Reveal Intimate Lifestyle or Biographical Details

92. With respect, yet putting it frankly, the majority of the Court of Appeal should not have found that this criterion supported a reasonable expectation of privacy, though its findings on the other points correctly resulted in a correct conclusion overall. The Crown commends to this Court Mr. Justice Ottenbreit's analysis, as well as his analysis in *R. v. Trapp.*

R. v. Trapp (2011), 377 Sask. R. 246 (C.A.), pars. 73 - 136

93. Is the subscriber information part of a "biographical core of personal information which individuals...wish to maintain and control from dissemination to the state", as explained in *Plant*? For that is a key part of the analysis, as Justice Deschamps put it in *Gomboc*:

> Thus, the fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative. Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved, the reasons why it was collected, and the circumstances in which it was intended to be used.
>
> *Gomboc, supra,* par. 34

94. The Crown says it is not core biographical data, let alone collected or kept for core privacy reasons. Instead, it is what is often referred to as 'tombstone' information. More than one court has seen it that way. There is *R. v. Wilson,* for example:

> In my view, the applicant had no reasonable expectation of privacy in the information provided by Bell considering the nature of that information. One's name and address or the name and address of your spouse are not "biographical information" one expects be kept private from the state. It is information available to anyone in a public directory and it does not reveal to use the words of Sopinka J. in *Plant* "intimate details of the lifestyle and personal choices or decisions of the applicant".
>
> *R. v. Wilson, supra,* par. 42; see also *R. v. Ewanyshyn*, unreported, March 29, 2009, (Alta. Q.B.), at par. 54; See also*: R. v. Friers*, 2008 CarswellOnt 6124 (C.J.)*; Ward, supra*; *R. v. Smith*, 2005 BCCA 334

95. Consider again *R. v. Pervez*, where the judge held that Mr. Pervez had no reasonable expectation of privacy in his sister's cell phone records, including her subscriber information:

> The records do not reveal intimate details of Pervez's lifestyle or personal choices. They merely show that a cell phone he used was in a certain place at a certain time and facilitated contact with another cell phone. The records only acquire significance when they are considered alongside the remaining evidence. The inferences provided by the records confirm the evidence of various witnesses, including that of Desmond Thomas, the driver of Debrocke's get-away vehicle.
>
> *R. v. Pervez, supra*, par. 12

96. Returning to *R. v. Gomboc* for a moment, one recalls that the information revealed the timing and extent of electrical usage. It said something, though a small something, about what was actually going on inside the home at specific times. Four justices held there was no reasonable expectation of privacy because of the information's "remoteness" from the "biographical core".

> *R. v. Gomboc, supra*, at par. 1 and par. 2, pars. 36 and 37

97. The information here did not identify the Appellant at all. It did not reveal who was on the internet at the time Det. Sgt. Parisien found the child pornography on offer, or that anyone was. It was just a name and address. It is a bit like a magazine subscription - learning a magazine is delivered to a particular person at a particular house does not say anything more than that - it does not even say whether the person reads the magazine, ornaments the coffee table with it, or what have you. The subscriber information had no tendency to reveal anything beyond the fact the Appellant's sister had contracted for an internet connection. The name and address of the subscriber gave the investigator no access to the computer(s) at the residence. They needed a warrant for that.

Gomboc, supra, pars. 7 and 8, par. 10 and par. 14

98. So how did the majority in the Court of Appeal go wrong on this point? With respect, in this case both Caldwell, J.A., and Cameron, J.A., erred in so far as they looked beyond the subscriber information and combined it with the police discovery of child pornography, the time of the discovery and so on, and then inferred things about what went on in the apartment from all the information. They also made the mistake of asking whether the subscriber information had the 'potential' to reveal intimate details (a perspective which invites such combining of information) instead of asking whether the information, in itself, 'tended' (the word used in *Plant*) to reveal personal details about the subscriber or anyone else in the residence.

Court of Appeal Reasons, Appellant's Record starting at page 28, pars. 22-28, and 98, *R. v. Trapp, supra,* pars. 27-41; See also *R. v. Ward, supra*, par. 93

99. The same error plagues the Appellant's argument. He points to how the subscriber information (wrongly referred to interchangeably as the "IP address") can lead the police to all kinds of information about a person's life, habits and preferences. Neither the evidence nor reason supports the assertion. He also says that the subscriber information can reveal so much about a person, which is a clear indication he is conflating the subscriber information with the child pornography, and with the computer which the investigator could not access without a warrant.

100. The Appellant's repeated references to this Court's decision in *Morelli* further evidences the Appellant's error. *Morelli* was about information inside a personal computer. This case is not about that. This case is the equivalent of asking a person to check their Rolodex for a name and address.

R. v. Morelli, [2010] 1 S.C.R. 253 - Appellant's Authorities, Tab 14

101. Subscriber information is actually less revealing than electrical consumption records (*Plant*) or heat signatures (*Tessling*). Subscriber information only shows the fact of a contract for an internet connection, something which is hardly a deep secret nowadays. Moreover, the subscriber information was of no real use unless judicial authorization granted police the power to search the residence. Judicial supervision at that stage ensured no prospect of abuse.

102. So, it seems, goes the thinking in the United States, too. There, "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation".

> *United States v. Perrine*, 518 F.3d 1196, 1204-1205 (10th Cir., 2008); See also: *United States v. Bynum*, 604 F.3d 162, 164-165 (4th Cir., 2010); and *United States v. Stults*, 575 F.3d 834, 842-843 (8th Cir., 2009)

103. The subscriber information here is the kind of information people give out every day. It is something typically given out on request. Other than permitting someone to wrongly judging another by the part of town in which they reside, it says nothing about a person. It is not core information.

(vii) The Circumstances Removed Any Expectation of Privacy

104. The Crown would add a consideration to the *Patrick* list. Unlike cases such as *Gomboc, Tessling*, and *Plant*, where there was nothing public about the activity, this case arises out of file sharing. That is a public activity, one open to anyone with the same or similar software. That is not to say that illegal activities are entitled to lesser privacy, or that public activities do not admit of privacy considerations. Rather, the point is that a reasonable person would expect citizens, the police, or the internet service provider to notice child pornography sharing and do something.

105. If someone set up a stand at a public market and left child pornography lying around, a reasonable person would expect someone to notice and the police to investigate. The police would no doubt arrest the individual at once. If the person who set up the stand was not around, though, the police would surely investigate, perhaps asking others at the market the identity and location of the stand's owner, or linking the stand to the vehicle that brought it to the market. Thus they would obtain an address by checking the vehicle licence plate and then get a warrant to the home. Again, it is not about the privacy of public activities, it is about the reasonable expectation that the people tasked with protecting society from crime would ask others to help by providing basic, identifying information and the expectation those others would cooperate. It is not decisive in itself, perhaps, but it is yet another consideration that plays against the Appellant's privacy claim.

D. There was No Reasonable Expectation of Privacy, so s. 8 Does Not Apply

106. The subscriber information obtained by police was of no use in itself. It did not permit the laying of a criminal charge or allow the child pornography investigator to search the location without judicial authorization. He needed to, and did, obtain a warrant before he was able to determine the extent of what had happened and who was responsible. As such, the real expectation of privacy was protected - judicial supervision was a condition precedent to obtaining core biographical information from the residence or any computers inside. What the Appellant would have this Court adopt is something of a *reductio ad absurdum*, for he would require a warrant to get enough information to get a search warrant. If there is anything unreasonable here, it is expecting that level of privacy.

107. Everything from the nature of the information to its distance from a person's biographical core, from the contractual terms to the bounds of privacy legislation, lead to the conclusion that a reasonable person would not expect privacy in this instance. That conclusion is wholly supported by the thinking in cases such as *Plant*, *Tessling*, *Gomboc* and *Ward*, and the thinking of Ottenbreit, J.A., in this case. There is no reasonable expectation of privacy. The possession conviction is sound.

II. If There was a Search, it was Reasonable

108. Even if there was a reasonable expectation of privacy here, it seems strange to call the letter the investigator sent to Shaw a search. It was a request for assistance, such as might be made of any bystander or potential witness. It was only an inquiry. Shaw could have refused. There was no forcible stripping of privacy. Certainly, there was no privilege involved here. However, this Court's decision in *R. v. Dersch*, and decisions in other cases, seem to say otherwise (*Dersch* saw doctor choose to answering a police inquiry about the accused's medical condition without the accused's consent, and the inquiry was termed "analogous to a search or a seizure"). If it is to be seen as a search, then, *R. v. Collins* established three hallmarks of a reasonable one: lawful authority to search; the reasonableness of that law; and the reasonableness of the search itself.

R. v. Dersch, [1993] 3 S.C.R. 768; *R. v. Collins*, [1987] 1 S.C.R. 265, par. 34

109. The Court of Appeal found, if there had been a reasonable expectation of privacy in the subscriber information so that the investigator's request of Shaw constituted a search, that search was reasonable. The Crown supports that conclusion and its underpinnings.

> *Court of Appeal Reasons, Appellant's Record starting at page 28,* pars. 46, 99 and 111*; R. v. Trapp,* pars. 66 through 71

110. As noted above, *PIPEDA* grants Shaw the right to share the information and the *Criminal Code* then gives the police the necessary authorization. Section 487.014 of the *Code* makes it lawful for the police to ask after any information another person is not prohibited by law from disclosing:

> 487.014(1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.
>
> (2) A person who provides documents, data or information in the circumstances referred to in subsection (1) is deemed to be authorized to do so for the purposes of section 25.

111. As a result, unless the desired information, documents or data cannot be released due to contractual terms, or unless there is a statute barring its revelation in the circumstances, the internet service provider may cooperate with the police upon receiving a request. For the reasons already stated, the contract between Shaw and the Appellant's sister allowed Shaw to disclose in the circumstances here.

112. With the overarching test for a lawful sharing under *PIPEDA* being whether it is 'reasonably appropriate' to do so, and with the contract's permissiveness clear, one must consider that the investigator was pursuing a child pornography matter. Equally, he sought minimal information: the name and address of the subscriber to a particular internet connection at a particular time. Det. Sgt. Parisien was not asking whether that subscriber was the one using the internet connection at the material time; indeed, he could not say who was doing so even after receiving the information from Shaw. He was not asking if it was the subscriber's computer which was hooked up to the internet, or asking for his internet or other history, and Shaw did not tell them that either (if it even could).

113. The reason for the request and the nature of the request were appropriate. It was reasonable for Shaw to assist. In addition, Shaw has a legitimate interest in preserving the integrity of its business by ensuring its internet service is used and perceived to be used only for lawful purposes. It cannot then be wrong for Shaw to give over information to the police only to help ferret out internet criminals, and thereby protect its own reputation. This, too, finds support in *Gomboc*, where, as stated, members of this Court recognized the company could do its own checks to determine if illegal activities were likely taking place in the home. Shaw did less here.

Gomboc, supra, par. 41; see also pars. 36 and par. 37

114. In *R. v. McNeice* German authorities notified the RCMP that someone using a British Columbia IP address had accessed child pornography. Investigating officers made a request of the internet service provider in accordance with subsection 7(3) of the *PIPEDA* for information which would identify the subscriber. Northwestel shared the information, which the investigators used to obtain a warrant authorizing a residential search and the seizure of his home computer.

R. v. Kelly Glenn McNeice, 2010 BCSC 1544, at pars. 5 through 15

115. Meiklem J. ruled, in part, that the joint operation of s. 487.014 of the *Criminal Code* and s. 7(3) of *PIPEDA* obviated the need for a warrant or production order. The judge recognized the independent agency of the service provider - and its right to decide whether or not to cooperate.

Ibid., pars. 40 through 45

116. So, the *Code* and *PIPEDA* authorized what happened here. The law was not challenged, let alone found unreasonable.

117. Turning to the last of the *Collins* criteria, the manner of search was as reasonable as could be. The letter to Shaw was clear and persuasive, while leaving it up to Shaw to decide whether or not to comply. The search took place in a location neither owned nor controlled by the Appellant. It involved the minimally intrusive provision of data that would likely be known to many people, and parameters of what was sought were highly constrained.

118. For all those reasons, and presuming a search took place, it was authorized by law and reasonably done.

III. If There was a s. 8 Violation, Section 24(2) Saves the Evidence

119. If, contrary to the foregoing submissions, this Court concludes that the Appellant had a reasonable expectation of privacy in the subscriber information and that section 8 of the *Charter* was violated by a simple request for the information, then this evidence should not be excluded. The trial judge did not consider the section 24(2) issue; however, this Court may adjudicate it as there is no dispute as to the facts.

120. As this Court has made clear, whether to exclude evidence turns on three considerations:

A. the seriousness of the *Charter*-infringing state conduct;

B. the impact of the *Charter*-protected interests of the accused; and

C. society's interest in an adjudication on the merits.

R. v. Grant, [2009] 2 S.C.R. 353, Appellant's Authorities, Tab 10, at par. 71

A. The Investigator's Relatively Innocuous Conduct Favours Admission

121. Conduct resulting in *Charter* violations may vary in seriousness; at one end of the spectrum are inadvertent or minor violations which minimally undermine public confidence in the rule of law, while at the other end is the willful and reckless disregard of *Charter* rights which inevitably has a negative effect. Also, this branch of the inquiry is meant to preserve public confidence in the rule of law and its processes, not punish the police. Good faith on the part of the police will reduce the need for the court to disassociate itself from any misconduct.

Ibid., at pars. 73-75

122. Here, Detective Sergeant Parisien obtaining the Appellant's sister's name and address from the corporate headquarters of Shaw is about the least intrusive violation of section 8 of the *Charter* imaginable given the contract and *PIPEDA*. The officer acted in good faith at all times - within the

bounds of many lower court decisions in a disputed area. Had the officer been required to obtain a production order or search warrant, there is no reason to doubt he would have done so.

B. The Minimal Impact on the Appellant's Interests Favours Admitting the Evidence

123. This branch of the section 24(2) inquiry requires an evaluation of the extent to which the breach actually undermined the interests protected by the *Charter* right infringed. The impact of the *Charter* breach may range from fleeting and technical to profoundly intrusive. An unreasonable search which intrudes on an area in which the Appellant enjoys a high expectation of privacy or which demeans his dignity is more serious than one which does not.

Ibid., at pars. 76-78

124. As already submitted, there was no intrusion to the Appellant's informational privacy. The request was focused and specific, limited as it was to a particular date and time. There was no interference with his territorial privacy, bodily integrity or right against self-incrimination.

C. Society's Interest in an Adjudication on the Merits Favours Admitting the Evidence

125. This third and final branch of the section 24(2) inquiry asks whether the truth-seeking function of a criminal trial is better served by the admission of the evidence over its exclusion. It reflects society's collective interest in ensuring that those who violate the law are brought to trial and their anti-social conduct adjudicated to determine whether it is criminal. The reliability of the evidence in question and its importance to the prosecution's case are important.

Ibid., at pars. 79-83

126. Certainly, the administration of justice would be negatively impacted by the exclusion of the subscriber information and the evidence gathered through the subsequent search warrant. The evidence is as reliable as can be and the case would fall without it. At the same time, the offences are insidious, including anonymously sharing child pornography with other members of the public, further perpetuating the exploitation of children, the most vulnerable members of society.

IV. The Court of Appeal Rightly Ordered a New Trial on the Making Available Offence

A. The Trial Judge Required a 'Positive Step' to Prove the Mental Element

127. The Appellant asserts that the trial judge did not require that a positive step be taken to make child pornography available before he would be prepared to find the mental element of the offence; instead, he was simply not satisfied without it. The judge's assertion that he did not think the Appellant 'knew' of the file sharing program making the child pornography available should therefore be inferred to mean that the judge considered wilful blindness, too.

128. The Court of Appeal disagreed, and so does the Crown. With respect, the trial judge looked at the matter too narrowly, and no attempt at rehabilitative reading of his judgment will change that.

129. In giving his decision, the learned trial judge held that the only way for the Crown to prove the making available crime was to prove that the Appellant had made an active effort to that end:

> At paragraph 36 of the *Morelli* decision the Court stated that to establish possession it must be shown that the file was knowingly stored and retained through the cache. And I won't bother going into what a cache is at this stage.
>
> The point here is, they imposed a *mens rea* test of knowingly. In my view as well, the specific intent of knowingly must also be shown with respect to the significant offence of making available as reflected in count 2. That making available must be shown to be part of a positive step or action before it can be said to meet that criteria.
>
> *Queen's Bench Reasons for Judgment, Appellant's Record, page 22 (596), line 21 - page 23 (597), line 7* (emphasis added)

130. The judge then emphasized his addition to both the *actus reus* and the *mens rea:*

> 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 *(sic)* as distribution under that particular section. If this were not the case, then having someone see a pornographic image of a child on your computer screen as you walk by would constitute distribution. That, in my view, does not reflect the legislative intent or the rationale for making it a one-year minimum sentence.
>
> The fact that all of these activities coupled within the general description at the beginning of the section of distribution, are supported by the elevated penalties, and supported by the elevated penalties *(sic)*, a clear indication of a greater societal approbation for that activity than for simple possession under the previous section. 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.
>
> *Ibid., page 23 (597), line 8 - page 24 (598), line 11*

131. As a result, the judge held that because the Appellant was passive - allowing the default setting on the computer to share files obtained through file sharing - he could not be found guilty:

> In this case Mr. Spencer did not take active facilitation steps that would serve as an indicator of intent. 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.
>
> From this I think it is very difficult to conclude that he had the knowing, live intention to distribute or make child pornography available to others. I am therefore left with a reasonable doubt from the entire evidence of the case as to whether Mr. Spencer meets the essential elements on count 2 of distribution and making available to find him guilty.
>
> *Ibid., page 25 (599), lines 6 - 22* (emphasis added)

132. While the Appellant argues that the phrase 'very difficult' means the judge did not make proof of an active step a prerequisite to a finding of the necessary *mens rea*, the phrase must be read in its full context. The judge called for a level of intent which could only be established by something more than passive sharing. His example set out above - that letting others see an image is not sufficient - and reading his reasons as a whole reveals that perspective.

133. The trial judge's use of the phrase "true awakening" answers the intention question completely. It indicates the judge required full knowledge before he would hold the *mens rea* proven. That fits with his requirement of an active step to demonstrate deliberate determination to make child pornography available.

B. The Judge was Wrong to Require a Positive Step

134. This was wrong for several reasons. First of all, despite the trial judge's attribution, it is without foundation in *Morelli* or any other case of which the Crown is aware. *Morelli* was about, in part, the difference between possession and accessing, rather than making child pornography available. *Morelli* turned on the issue of whether viewing child pornography over the internet was

done with sufficient knowledge and control that a person could be said to go beyond the crime of accessing to the point of legal possession.

R. v. Morelli, supra

135. Secondly, it equates distribution and making available. Consider the judge's error in the preceding quotes, where he mistakenly uses the word "distribution" - another, separate means of committing an offence under the section and something not charged - instead of 'making available'.

136. The trial judge also erred with his hypothetical, for he states he did not see how something so passive could attract liability because it would mean someone who watched child pornography where others could happen by and see it was guilty of making available of child pornography. Yet that is very much the kind of crime making available is.

137. With respect, the trial judge missed the very point of the making available offence. Distribution or advertising is the relatively active crime. Making available is the comparatively passive crime - keeping or letting the material lay where it can be seen or taken by others. It is about child pornography left available or shown to people in settings that are not distribution, advertising or the other active methods. If one were to look at child pornography on the computer, with one's computer screen just so happening to face the open door of one's office, in circumstances where passers by would be expected and would see the images, how is that *not* making available?

138. *R. v. Mallory*, a judgment from the Ontario Superior Court, supports this. In that case, the defence argued that simply leaving material in the shared folder did not amount to "making available". The judge disagreed:

> By leaving the offending material in a shared file the accused knew others had access to child pornography and the elements of the offence have been established. No further positive act need have been taken. In fact, the act of deleting them or removing them from a shared account was necessary to prevent them from being "made available". "Transmitting" or "Distributing" are separate acts prohibited by the same section.
>
> *R. v. Mallory* (2008), Unreported, File 10174 (Ont. S.C.J.) at par. 24; see also *R. v. Johannson* (2008), 335 Sask. R. 22 (Q.B.), at pars. 34 - 36; and *R. v. Pressacco* (2010), 2010 CarswellSask 193, at pars. 29 and 30 (where passive sharing sufficed as long as it was more than transient - the Crown considers even transient sharing sufficient).

139. What seems to have happened in the present case is a melding of motive, *actus reus*, *mens rea*, and the different crimes under the section. That was wrong, and it led the judge to require full, actual knowledge before he would convict.

C. The Error Led to the Judge Ignoring the Prospect of Wilful Blindness

140. The judge's requirement for some positive step to make out the offence ruled out the prospect of wilful blindness as part of the *mens rea*. That calls for the new trial the Court of Appeal ordered.

141. The intent for a crime committed "knowingly", as this one must be, is that the person mean to do it or else be wilfully blind or reckless as to such knowledge.

R. v. Sault Ste. Marie (City), [1978] 2 S.C.R. 1299, pages 1309-10

142. Wilful blindness does not presuppose actual knowledge. Instead, it is the avoidance of that knowledge once suspicion is raised, the suppressing of suspicion.

R. v. Briscoe, [2010] 1 S.C.R. 411, pars 21 through 23

143. Wilful blindness applies to child pornography offences.

R. v. Dixon (2005), 2005 CarswellNat 400 (Court Martial Appeal Court), par. 9

144. Even in light of the judge's erroneous call for a 'positive step' as part of the offence, the Crown recognizes it is left with the judge's factual finding that the Appellant did not "know" he was file sharing. The finding really leaves no room for argument about actual knowledge or subjective recklessness. Yet, the judge's finding does not resolve whether the Appellant did not know because he had closed his eyes to suspicions he held.

Queen's Bench Reasons for Judgment, Appellant's Record, page 21 (595), lines 2 - 5

145. While the Crown argued wilful blindness at trial, defence counsel at trial suggested it did not even figure in the offence. The Judge's requirement of an active element precluded it, at the very least.

Transcript, Arguments, pages 532 and 581; *R. v. Briscoe, supra*, par. 11 and the result (a new trial)

146. The trial judge's call for a positive act before he would find guilt is definitive, but there is also the judge's failure to deal with so much evidence of wilful blindness, as outlined in the factual portion of this factum. To repeat just one, there is evidence from the Appellant confirming that he actually had suspicions. Note the past tense of his admission:

> P I mean I never even thought that's a bogus answer. You never thought about that (sic) the fact that you're on a file sharing program, that you're sharing files? You got to be kidding me?
>
> S Well, I knew I was, like I guess I just never, I just [see it as](inaudible)
>
> P I'll maybe put it to you this way, you didn't really care. OK, cause there's no way you didn't know it was happening. There's no way you, there's nothing you did to stop it from happening, you could have disconnected, you could have shut down all of your Limewire and just gone with what you had, but, the real answer is you didn't care.
>
> S Which is just sick, but it's true.

Warned Statement, supra, page 43, lines 11 - 20; Queen's Bench Reasons for Judgment, Appellant's Record, page 24 (598), line 12, through page 25 (599), line 12

That answer was not qualified or related to some sudden awareness in the course of the police interview, and it only makes sense if it speaks to the state of mind while possessing and sharing.

147. The judge did not address those comments at all, or the rest of the evidence. The judge did not address the prospect that even if the Appellant did not *know* he was sharing, the Appellant at least ignored his own suspicions.

D. The Court of Appeal was Correct to Order a New Trial

148. That the judge required a "positive step" as part of making child pornography available calls for correction. His consequent failure to consider wilful blindness as a path to conviction, and to consider the evidence in support of finding wilful blindness, also calls for correction. If his decision stands, it could be interpreted as saying that simply leaving child pornography in a shared folder, or elsewhere, available to others, is never an offence. That is wrong, and ordering a new trial says so.

IV. No Reasonable Expectation of Privacy; The Need to Consider Wilful Blindness

149. There is no reasonable expectation of privacy in a person's name and address given to an internet service provider. There is certainly no such expectation when the internet service contract and *PIPEDA* allow for disclosure, and the police would have to get a search warrant to do anything useful with the information. All the less so when the person is sharing files with the world. As to the offence of making child pornography available, a person does not have to do something active to commit it and wilful blindness is part of the intent.

PART IV

SUBMISSIONS AS TO COSTS

150. The Respondent submits that this Honourable Court should not make an order as to costs. The Appellant has not sought them and there is nothing about this case which would warrant them.

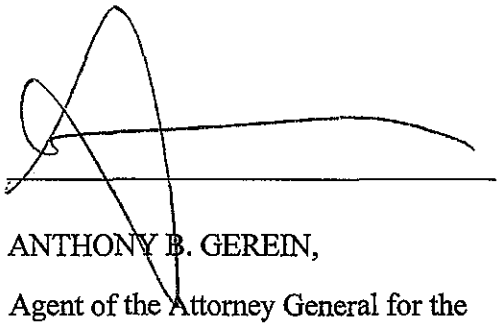
PART V

NATURE OF THE ORDER SOUGHT

151. The Respondent requests that this Honourable Court dismiss the appeal.

ALL OF WHICH is respectfully submitted.

DATED at the City of Regina, in the Province of Saskatchewan, this 7th day of July, A.D. 2013.



ANTHONY B. GEREIN,

Agent of the Attorney General for the Province of Saskatchewan

PART VI

TABLE OF AUTHORITIES

PART VII
LEGISLATION

Personal Information Protection and Electronic Documents Act

S.C. 2000, c. 5

Assented to 2000-04-13

Loi sur la protection des renseignements personnels et les documents électroniques

L.C. 2000, ch. 5

Sanctionnée 2000-04-13

Purpose

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances

Objet

3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Application

4. (1) This Part applies to every organization in respect of personal information that

(*a*) the organization collects, uses or discloses in the course of commercial activities; or

(*b*) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Marginal note:Limit

(2) This Part does not apply to

(*a*) any government institution to which the Privacy Act applies;

(*b*) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or

(*c*) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

Marginal note: Other Acts

(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.

[Note: Subsection 4(3) in force January 1, 2001, *see* SI/2000-29.]

Champ d'application

4. (1) La présente partie s'applique à toute organisation à l'égard des renseignements personnels :

a) soit qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales;

b) soit qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre d'une entreprise fédérale.

Note marginale :Limite

(2) La présente partie ne s'applique pas :

a) aux institutions fédérales auxquelles s'applique la Loi sur la protection des renseignements personnels;

b) à un individu à l'égard des renseignements personnels qu'il recueille, utilise ou communique à des fins personnelles ou domestiques et à aucune autre fin;

c) à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique à des fins journalistiques, artistiques ou littéraires et à aucune autre fin.

Note marginale :Autre loi

(3) Toute disposition de la présente partie s'applique malgré toute disposition — édictée après l'entrée en vigueur du présent paragraphe — d'une autre loi fédérale, sauf dérogation expresse de la disposition de l'autre loi.

Retour la référence de la note de bas de page *[Note : Paragraphe 4(3) en vigueur le 1er janvier 2001, *voir* TR/2000-29.]

2.....

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

2....

« organisation » S'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales.

Collection without knowledge or consent

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

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

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

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

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

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

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

(ii) that is required by law.

Marginal note:Use without knowledge or consent

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

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

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

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

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

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

Marginal note:Disclosure without knowledge or consent

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

(*a*) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(*b*) for the purpose of collecting a debt owed by the individual to the organization;

(*c*) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(*c.1*) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

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

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

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

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

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

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

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

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

(*e*) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in

writing without delay of the disclosure;

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

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

(*h*) made after the earlier of

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

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

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

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

(*i*) required by law.

Marginal note:Use without consent

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

Marginal note:Disclosure without consent

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

2000, c. 5, s. 7, c. 17, s. 97; 2001, c. 41, s. 81; 2004, c. 15, s. 98.

Collecte à l'insu de l'intéressé et sans son consentement

7. (1) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut recueillir de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) la collecte du renseignement est manifestement dans l'intérêt de l'intéressé et le consentement ne peut être obtenu auprès de celui-ci en temps opportun;

b) il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé puisse compromettre l'exactitude du renseignement ou l'accès à celui-ci, et la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;

c) la collecte est faite uniquement à des fins journalistiques, artistiques ou littéraires;

d) il s'agit d'un renseignement réglementaire auquel le public a accès;

e) la collecte est faite en vue :

(i) soit de la communication prévue aux sous-alinéas (3)*c.1*)(i) ou *d*)(ii),

(ii) soit d'une communication exigée par la loi.

Note marginale :Utilisation à l'insu de l'intéressé et sans son consentement

(2) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut utiliser de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) dans le cadre de ses activités, l'organisation découvre l'existence d'un renseignement dont elle a des motifs raisonnables de croire qu'il pourrait être utile à une enquête sur une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être, et l'utilisation est faite aux fins d'enquête;

b) l'utilisation est faite pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité de tout individu;

c) l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites, ces fins ne peuvent être réalisées sans que le renseignement soit utilisé, celui-ci est utilisé d'une manière qui en assure le caractère confidentiel, le consentement est pratiquement impossible à obtenir et l'organisation informe le commissaire de l'utilisation avant de la faire;

c.1) il s'agit d'un renseignement réglementaire auquel le public a accès;

d) le renseignement a été recueilli au titre des alinéas (1)*a*), *b*) ou *e*).

Note marginale :Communication à l'insu de l'intéressé et sans son consentement

(3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

a) la communication est faite à un avocat — dans la province de Québec, à un avocat ou à un notaire — qui représente l'organisation;

b) elle est faite en vue du recouvrement d'une créance que celle-ci a contre l'intéressé;

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

c.1) elle est faite à une institution gouvernementale — ou à une subdivision d'une telle institution — qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas :

(i) qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales,

(ii) que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application,

(iii) qu'elle est demandée pour l'application du droit canadien ou provincial;

c.2) elle est faite au titre de l'article 7 de la **Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes** à l'institution gouvernementale mentionnée à cet article;

Note de bas de page *c.2*) elle est faite au titre de l'article 7 de la Loi sur le recyclage des produits de la criminalité à l'institution gouvernementale mentionnée à cet article;

Retour à la référence de la note de bas de page [Note : L'alinéa 7(3)*c.2*), édicté par l'alinéa 97(1)*a*) du chapitre 17 des Lois du Canada (2000), sera abrogé ultérieurement.]

d) elle est faite, à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et l'organisation, selon le cas, a des motifs raisonnables de croire que le

renseignement est afférent à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être ou soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;

e) elle est faite à toute personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne et, dans le cas où la personne visée par le renseignement est vivante, l'organisation en informe par écrit et sans délai cette dernière;

f) elle est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites, ces fins ne peuvent être réalisées sans que le renseignement soit communiqué, le consentement est pratiquement impossible à obtenir et l'organisation informe le commissaire de la communication avant de la faire;

g) elle est faite à une institution dont les attributions comprennent la conservation de documents ayant une importance historique ou archivistique, en vue d'une telle conservation;

h) elle est faite cent ans ou plus après la constitution du document contenant le renseignement ou, en cas de décès de l'intéressé, vingt ans ou plus après le décès, dans la limite de cent ans;

h.1) il s'agit d'un renseignement réglementaire auquel le public a accès;

h.2) elle est faite par un organisme d'enquête et est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;

i) elle est exigée par la loi.

Note marginale :Utilisation sans le consentement de l'intéressé

(4) Malgré l'article 4.5 de l'annexe 1, l'organisation peut, dans les cas visés au paragraphe (2), utiliser un renseignement personnel à des fins autres que celles auxquelles il a été recueilli.

Note marginale :Communication sans le consentement de l'intéressé

(5) Malgré l'article 4.5 de l'annexe 1, l'organisation peut, dans les cas visés aux alinéas (3)*a*) à *h.2*), communiquer un renseignement personnel à des fins autres que celles auxquelles il a été recueilli.

2000, ch. 5, art. 7, ch. 17, art. 97; 2001, ch. 41, art. 81; 2004, ch. 15, art. 98.

SCHEDULE 1

(Section 5)

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

4.3 Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

ANNEXE 1

(article 5)

PRINCIPES ÉNONCÉS DANS LA NORME NATIONALE DU CANADA INTITULÉE *CODE TYPE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*, CAN/CSA-Q830-96

4.3 Troisième principe — Consentement

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins du contrôle d'application de la loi, de la détection d'une fraude ou de sa prévention, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une oeuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels.

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.

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. 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.

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.