Matthew David Spencer *Appellant*

v.

Her Majesty The Queen *Respondent*

and

Director of Public Prosecutions, Attorney General of Ontario, Attorney General of Alberta, Privacy Commissioner of Canada, Canadian Civil Liberties Association and Criminal Lawyers' Association of Ontario *Interveners*

Matthew David Spencer *Appelant*

c.

Sa Majesté la Reine *Intimée*

et

Directeur des poursuites pénales, procureur général de l'Ontario, procureur général de l'Alberta, commissaire à la protection de la vie privée du Canada, Association canadienne des libertés civiles et Criminal Lawyers' Association of Ontario *Intervenants*

Indexed as: R. *v.* Spencer

2014 SCC 43

File No.: 34644.

2013: December 9; 2014: June 13.*

Present: McLachlin C.J. and LeBel, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis and Wagner JJ.

Répertorié : R. *c.* Spencer

2014 CSC 43

N° du greffe : 34644.

2013 : 9 décembre; 2014 : 13 juin*.

Présents : La juge en chef McLachlin et les juges LeBel, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis et Wagner.

ON APPEAL FROM THE COURT OF APPEAL FOR SASKATCHEWAN

Constitutional law — Charter of Rights — Search and seizure — Privacy — Police having information that IP address used to access or download child pornography — Police asking Internet service provider to voluntarily provide name and address of subscriber assigned to IP address — Police using information to obtain search warrant for accused's residence — Whether police conducted unconstitutional search by obtaining subscriber information matching IP address — Whether evidence obtained as a result should be excluded — Whether fault element of making child pornography available requires proof of positive facilitation — Criminal Code, R.S.C. 1985, c. C-46, ss. 163.1(3), (4), 487.014(1) — Personal Information Protection and Electronic Documents Act,

EN APPEL DE LA COUR D'APPEL DE LA SASKATCHEWAN

Droit constitutionnel — Charte des droits — Fouilles, perquisitions et saisies — Protection des renseignements personnels — Police détenant des renseignements selon lesquels une adresse IP a été utilisée pour avoir accès à de la pornographie juvénile ou pour la télécharger — Demande de la police au fournisseur de services Internet de lui fournir volontairement le nom et l'adresse de l'abonnée à qui appartient l'adresse IP — Utilisation de ces renseignements par la police pour obtenir un mandat lui permettant de perquisitionner dans la résidence de l'accusé — La police a-t-elle effectué une fouille ou une perquisition inconstitutionnelle lorsqu'elle a obtenu les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP? — La preuve ainsi obtenue devrait-elle être

* A motion to amend the reasons was granted on November 6, 2014, amending para. 12. The amendments are included in these reasons.

* Une requête en modification des motifs a été accordée le 6 novembre 2014 modifiant le par. 12. Les modifications ont été incorporées dans les présents motifs.

S.C. 2000, c. 5, s. 7(3)(c.1)(ii) — Canadian Charter of Rights and Freedoms, s. 8.

écartée? — L'élément de faute de l'infraction qui consiste à rendre accessible la pornographie juvénile exige-t-il la preuve d'un appui délibéré? — Code criminel, L.R.C. 1985, ch. C-46, art. 163.1(3), (4), 487.014(1) — Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 7(3)c.1)(ii) — Charte canadienne des droits et libertés, art. 8.

The police identified the Internet Protocol (IP) address of a computer that someone had been using to access and store child pornography through an Internet file-sharing program. They then obtained from the Internet Service Provider (ISP), without prior judicial authorization, the subscriber information associated with that IP address. The request was purportedly made pursuant to s. 7(3)(*c.*1)(ii) of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). This led them to the accused. He had downloaded child pornography into a folder that was accessible to other Internet users using the same file-sharing program. He was charged and convicted at trial of possession of child pornography and acquitted on a charge of making it available. The Court of Appeal upheld the conviction, however set aside the acquittal on the making available charge and ordered a new trial.

La police a découvert l'adresse de protocole Internet (IP) de l'ordinateur qu'une personne avait utilisé pour accéder à de la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de fichiers. Elle a ensuite obtenu auprès du fournisseur de services Internet (FSI), sans autorisation judiciaire préalable, les renseignements relatifs à l'abonnée à qui appartenait cette adresse IP. Il s'agit d'une demande qui aurait été fondée sur le sous-al. 7(3)*c.*1)(ii) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDE*). Les policiers ont ainsi découvert l'accusé. Celui-ci avait téléchargé de la pornographie juvénile à partir d'Internet avant de sauvegarder les fichiers en question dans un répertoire qui était accessible à d'autres internautes utilisateurs du même programme de partage de fichiers. L'accusé a été inculpé et déclaré coupable au procès de possession de pornographie juvénile, mais il a été acquitté de l'accusation de la rendre accessible. La Cour d'appel a confirmé la déclaration de culpabilité; elle a cependant annulé l'acquittement et ordonné la tenue d'un nouveau procès.

Held: The appeal should be dismissed.

Arrêt : Le pourvoi est rejeté.

Whether there is a reasonable expectation of privacy in the totality of the circumstances is assessed by considering and weighing a large number of interrelated factors. The main dispute in this case turns on the subject matter of the search and whether the accused's subjective expectation of privacy was reasonable. The two circumstances relevant to determining the reasonableness of his expectation of privacy in this case are the nature of the privacy interest at stake and the statutory and contractual framework governing the ISP's disclosure of subscriber information.

On détermine s'il existe une attente raisonnable en matière de respect de la vie privée, compte tenu de l'ensemble des circonstances, en examinant et en soupesant un grand nombre de facteurs interreliés. Dans la présente affaire, le litige porte principalement sur l'objet de la fouille ou de la perquisition et sur la question de savoir si l'attente subjective de l'accusé en matière de vie privée était raisonnable. Les deux éléments pertinents pour déterminer le caractère raisonnable de son attente au respect de sa vie privée sont, d'une part, la nature de l'intérêt en matière de vie privée qui est en jeu et, d'autre part, le cadre législatif et contractuel régissant la communication par le FSI des renseignements relatifs à l'abonnée.

When defining the subject matter of a search, courts have looked not only at the nature of the precise information sought, but also at the nature of the information that it reveals. In this case, the subject matter of the search was not simply a name and address of someone in a contractual relationship with the ISP. Rather, it was the

Pour définir l'objet d'une fouille ou d'une perquisition, les tribunaux examinent non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés. En l'espèce, la fouille ou la perquisition n'avait pas simplement pour objet le nom et l'adresse d'une personne qui était liée

identity of an Internet subscriber which corresponded to particular Internet usage.

The nature of the privacy interest engaged by the state conduct turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought. In this case, the primary concern is with informational privacy. Informational privacy is often equated with secrecy or confidentiality, and also includes the related but wider notion of control over, access to and use of information. However, particularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating to an individual's identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. In this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests.

There is no doubt that the contractual and statutory framework may be relevant to, but not necessarily determinative of, whether there is a reasonable expectation of privacy. In this case, the contractual and statutory frameworks overlap and the relevant provisions provide little assistance in evaluating the reasonableness of the accused's expectation of privacy. Section 7(3)(*c.*1)(ii) of *PIPEDA* cannot be used as a factor to weigh against the

par contrat au FSI. Il s'agissait plutôt de l'identité d'une abonnée aux services Internet à qui correspondait une utilisation particulière de ces services.

La nature de l'intérêt en matière de vie privée visé par l'action de l'État tient au caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi qu'aux conséquences de cette dernière pour la personne qui en fait l'objet, et non à la nature légale ou illégale de la chose recherchée. En l'espèce, on s'intéresse principalement au caractère privé des renseignements personnels. Ce dernier est souvent assimilé à la confidentialité. Il comprend également la notion connexe, mais plus large, de contrôle sur l'accès à l'information et sur l'utilisation des renseignements. L'anonymat en tant que facette du droit à la vie privée revêt cependant une importance particulière dans le contexte de l'utilisation d'Internet. Il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de téléphone qui figurent parmi les renseignements relatifs à l'abonné. En établissant un lien entre des renseignements particuliers et une personne identifiable, les renseignements relatifs à l'abonné peuvent compromettre les droits en matière de vie privée quant à l'identité d'une personne en tant que source, possesseur ou utilisateur des renseignements visés. Un certain degré d'anonymat est propre à beaucoup d'activités menées sur Internet et l'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives. En l'espèce, la demande de la police, dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée, visait en fait à établir un lien entre une personne précise et des activités en ligne précises. Ce genre de demande concerne, en ce qui a trait aux renseignements personnels, le droit à la vie privée relatif à l'anonymat puisqu'elle vise à établir un lien entre le suspect et des activités entreprises en ligne sous le couvert de l'anonymat, activités qui, comme on l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en matière de vie privée.

Il ne fait aucun doute que les cadres législatif et contractuel peuvent aussi être pertinents, mais pas nécessairement déterminants, quant à la question de savoir s'il existe une attente raisonnable en matière de vie privée. En l'espèce, les cadres contractuel et législatif se chevauchent et les dispositions applicables ne sont guère utiles pour évaluer le caractère raisonnable de l'attente de l'accusé au respect de sa vie privée. Le sous-al. 7(3)*c.*1)(ii)

existence of a reasonable expectation of privacy since the proper interpretation of the relevant provision itself depends on whether such a reasonable expectation of privacy exists. It would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent. The contractual provisions in this case support the existence of a reasonable expectation of privacy. The request by the police had no lawful authority in the sense that while the police could ask, they had no authority to compel compliance with that request. In the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. Therefore, the request by the police that the ISP voluntarily disclose such information amounts to a search.

Whether the search in this case was lawful will be dependent on whether the search was authorized by law. Neither s. 487.014(1) of the *Criminal Code*, nor *PIPEDA* creates any police search and seizure powers. Section 487.014(1) is a declaratory provision that confirms the existing common law powers of police officers to make enquiries. *PIPEDA* is a statute whose purpose is to increase the protection of personal information. Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, the police do not gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information. The conduct of the search in this case therefore violated the *Charter*. Without the subscriber information obtained by the police, the warrant could not have been obtained. It follows that if that information is excluded from consideration as it must be because it was unconstitutionally obtained, there were not adequate grounds to sustain the issuance of the warrant and the search of the residence was therefore unlawful and violated the *Charter*.

de la *LPRPDE* ne peut être considéré comme un des facteurs défavorables à l'existence d'une attente raisonnable en matière de vie privée puisque l'interprétation juste de la disposition applicable dépend elle-même de l'existence d'une telle attente raisonnable en matière de vie privée. Il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou n'écarte pas l'interdiction générale prévue par la *LPRPDE* quant à la communication de renseignements personnels sans le consentement de l'intéressé. Les dispositions du contrat en l'espèce justifient l'existence d'une attente raisonnable en matière de vie privée. La demande de renseignements n'était pas étayée par la source de l'autorité légitime de la police, en ce sens que cette dernière pouvait formuler une demande, mais ne détenait pas l'autorité pour obliger le fournisseur à s'y conformer. Compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La demande faite par la police visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille.

La question de savoir si la fouille effectuée en l'espèce était légitime est subordonnée à celle de savoir si elle était autorisée par la loi. Ni le par. 487.014(1) du *Code criminel*, ni la *LPRPDE* n'ont pour effet de conférer à la police des pouvoirs en matière de fouilles, de perquisitions ou de saisies. Le paragraphe 487.014(1) est une disposition déclaratoire qui confirme les pouvoirs de common law permettant aux policiers de formuler des questions. La *LPRPDE* est une loi qui a pour objet d'accroître la protection des renseignements personnels. Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée en l'absence de circonstances contraignantes ou d'une loi qui n'a rien d'abusif, ils ne peuvent obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels. L'exécution de la fouille ou de la perquisition en l'espèce violait donc la *Charte*. Si les renseignements relatifs à l'abonnée ne lui avaient pas été communiqués, la police n'aurait pas pu obtenir le mandat. Par conséquent, si ces renseignements sont écartés (ce qui doit être le cas, parce qu'ils ont été obtenus d'une façon inconstitutionnelle), il n'y avait aucun motif valable justifiant la délivrance d'un mandat. La fouille ou la perquisition à la résidence était donc abusive et violait la *Charte*.

The police, however, were acting by what they reasonably thought were lawful means to pursue an important law enforcement purpose. The nature of the police conduct in this case would not tend to bring the administration of justice into disrepute. While the impact of the *Charter*-infringing conduct on the *Charter*-protected interests of the accused weighs in favour of excluding the evidence, the offences here are serious. Society has a strong interest in the adjudication of the case and also in ensuring the justice system remains above reproach in its treatment of those charged with these serious offences. Balancing the three factors, the exclusion of the evidence rather than its admission would bring the administration of justice into disrepute. The admission of the evidence is therefore upheld.

There is no dispute that the accused in a prosecution under s. 163.1(3) of the *Criminal Code* must be proved to have had knowledge that the pornographic material was being made available. This does not require however, that the accused must knowingly, by some positive act, facilitate the availability of the material. The offence is complete once the accused knowingly makes pornography available to others. Given that wilful blindness was a live issue and that the trial judge's error in holding that a positive act was required to meet the *mens rea* component of the making available offence resulted in his not considering the wilful blindness issue, the error could reasonably be thought to have had a bearing on the trial judge's decision to acquit. The order for a new trial is affirmed.

Cases Cited

Referred to: *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403; *McInerney v. MacDonald*, [1992] 2 S.C.R. 138; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wise*, [1992] 1 S.C.R. 527; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657; *R. v. Collins*, [1987] 1 S.C.R. 265;

Les policiers se sont toutefois servi de ce qu'ils croyaient raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Par sa nature, la conduite des policiers en l'espèce ne serait pas susceptible de déconsidérer l'administration de la justice. Bien que l'incidence de la conduite attentatoire sur les droits de l'accusé garantis par la *Charte* favorise l'exclusion de la preuve, les infractions reprochées en l'espèce sont graves. La société a un intérêt manifeste à ce que l'affaire soit jugée et à ce que le fonctionnement du système de justice demeure irréprochable au regard des individus accusés de ces infractions graves. Une mise en balance de ces trois facteurs permet de conclure que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice. L'admission de la preuve est donc confirmée.

Il n'est pas contesté que, dans le cadre d'une poursuite sous le régime du par. 163.1(3) du *Code criminel*, il faut prouver que l'accusé avait connaissance du fait que le matériel pornographique était rendu accessible à d'autres personnes. Il n'est toutefois pas nécessaire que l'accusé doive sciemment, par une certaine action délibérée, faciliter l'accessibilité au matériel. Les éléments de l'infraction sont tous réunis lorsque l'accusé rend sciemment la pornographie accessible à d'autres personnes. Puisque l'aveuglement volontaire était une question en litige et que l'erreur du juge du procès — lorsqu'il a conclu qu'il était nécessaire d'accomplir une action délibérée pour satisfaire à l'exigence de la *mens rea* de l'infraction de rendre accessible — lui a fait omettre l'examen de cette question, il serait raisonnable de penser que cette erreur a eu une incidence sur le verdict d'acquittement. L'ordonnance prescrivant la tenue d'un nouveau procès est confirmée.

Jurisprudence

Arrêts mentionnés : *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321; *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Dyment*, [1988] 2 R.C.S. 417; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211; *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246; *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456; *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569; *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403; *McInerney c. MacDonald*, [1992] 2 R.C.S. 138; *R. c. Duarte*, [1990] 1 R.C.S. 30; *R. c. Wise*, [1992] 1 R.C.S. 527; *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S.

R. v. McNeice, 2010 BCSC 1544 (CanLII); *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Briscoe*, 2010 SCC 13, [2010] 1 S.C.R. 411; *R. v. Graveline*, 2006 SCC 16, [2006] 1 S.C.R. 609.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).
Criminal Code, R.S.C. 1985, c. C-46, ss. 163.1(3), (4), 487.014.
Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01, s. 29(2)(g).
Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 3, 5(3), 7, Sch. 1, cl. 4.3.

Authors Cited

Canada. Report of the Task Force established by the Department of Communications/Department of Justice. *Privacy and Computers*. Ottawa: Information Canada, 1972.
Gleicher, Nathaniel. "Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web" (2009), 118 *Yale L.J.* 1945.
Gutterman, Melvin. "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988), 39 *Syracuse L. Rev.* 647.
Hubbard, Robert W., Peter DeFreitas and Susan Magotiaux. "The Internet — Expectations of Privacy in a New Context" (2002), 45 *Crim. L.Q.* 170.
Hunt, Chris D. L. "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011), 37 *Queen's L.J.* 167.
Paton-Simpson, Elizabeth. "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000), 50 *U.T.L.J.* 305.
Slane, Andrea, and Lisa M. Austin. "What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011), 57 *Crim. L.Q.* 486.
Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1970.

APPEAL from a judgment of the Saskatchewan Court of Appeal (Cameron, Ottenbreit and Caldwell JJ.A.), 2011 SKCA 144, 377 Sask. R. 280, 528 W.A.C. 280, [2012] 4 W.W.R. 425, 283 C.C.C. (3d) 384, [2011] S.J. No. 729 (QL), 2011 CarswellSask 786, affirming the accused's conviction for

657; *R. c. Collins*, [1987] 1 R.C.S. 265; *R. c. McNeice*, 2010 BCSC 1544 (CanLII); *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353; *R. c. Briscoe*, 2010 CSC 13, [2010] 1 R.C.S. 411; *R. c. Graveline*, 2006 CSC 16, [2006] 1 R.C.S. 609.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 8, 24(2).
Code criminel, L.R.C. 1985, ch. C-46, art. 163.1(3), (4), 487.014.
Freedom of Information and Protection of Privacy Act, S.S. 1990-91, ch. F-22.01, art. 29(2)(g).
Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 3, 5(3), 7, ann. 1, art. 4.3.

Doctrine et autres documents cités

Canada. Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. *L'ordinateur et la vie privée*. Ottawa : Information Canada, 1972.
Gleicher, Nathaniel. « Neither a Customer Nor a Subscriber Be : Regulating the Release of User Information on the World Wide Web » (2009), 118 *Yale L.J.* 1945.
Gutterman, Melvin. « A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance » (1988), 39 *Syracuse L. Rev.* 647.
Hubbard, Robert W., Peter DeFreitas and Susan Magotiaux. « The Internet — Expectations of Privacy in a New Context » (2002), 45 *Crim. L.Q.* 170.
Hunt, Chris D. L. « Conceptualizing Privacy and Elucidating its Importance : Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011), 37 *Queen's L.J.* 167.
Paton-Simpson, Elizabeth. « Privacy and the Reasonable Paranoid : The Protection of Privacy in Public Places » (2000), 50 *U.T.L.J.* 305.
Slane, Andrea, and Lisa M. Austin. « What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations » (2011), 57 *Crim. L.Q.* 486.
Westin, Alan F. *Privacy and Freedom*. New York : Atheneum, 1970.

POURVOI contre un arrêt de la Cour d'appel de la Saskatchewan (les juges Cameron, Ottenbreit et Caldwell), 2011 SKCA 144, 377 Sask. R. 280, 528 W.A.C. 280, [2012] 4 W.W.R. 425, 283 C.C.C. (3d) 384, [2011] S.J. No. 729 (QL), 2011 CarswellSask 786, qui a confirmé la déclaration de culpabilité

possession of child pornography and setting aside the accused's acquittal for making available child pornography entered by Foley J., 2009 SKQB 341, 361 Sask. R. 1, [2009] S.J. No. 798 (QL), 2009 CarswellSask 905, and ordering a new trial. Appeal dismissed.

Aaron A. Fox, *Q.C.*, and *Darren Kraushaar*, for the appellant.

Anthony B. Gerein, for the respondent.

Ronald C. Reimer and *David Schermbrucker*, for the intervener the Director of Public Prosecutions.

Susan Magotiaux and *Allison Dellandrea*, for the intervener the Attorney General of Ontario.

Jolaine Antonio, for the intervener the Attorney General of Alberta.

Mahmud Jamal, *Patricia Kosseim*, *Daniel Caron* and *Sarah Speevak*, for the intervener the Privacy Commissioner of Canada.

Anil K. Kapoor and *Lindsay L. Daviau*, for the intervener the Canadian Civil Liberties Association.

Jonathan Dawe and *Jill R. Presser*, for the intervener the Criminal Lawyers' Association of Ontario.

The judgment of the Court was delivered by

CROMWELL J. —

I. Introduction

[1] The Internet raises a host of new and challenging questions about privacy. This appeal relates to one of them.

[2] The police identified the Internet Protocol (IP) address of a computer that someone had been

de l'accusé quant à l'infraction de possession de pornographie juvénile et annulé son acquittement quant à l'infraction de rendre accessible la pornographie juvénile prononcés par le juge Foley, 2009 SKQB 341, 361 Sask. R. 1, [2009] S.J. No. 798 (QL), 2009 CarswellSask 905, et ordonné la tenue d'un nouveau procès. Pourvoi rejeté.

Aaron A. Fox, *c.r.*, et *Darren Kraushaar*, pour l'appelant.

Anthony B. Gerein, pour l'intimée.

Ronald C. Reimer et *David Schermbrucker*, pour l'intervenant le directeur des poursuites pénales.

Susan Magotiaux et *Allison Dellandrea*, pour l'intervenant le procureur général de l'Ontario.

Jolaine Antonio, pour l'intervenant le procureur général de l'Alberta.

Mahmud Jamal, *Patricia Kosseim*, *Daniel Caron* et *Sarah Speevak*, pour l'intervenant le commissaire à la protection de la vie privée du Canada.

Anil K. Kapoor et *Lindsay L. Daviau*, pour l'intervenante l'Association canadienne des libertés civiles.

Jonathan Dawe et *Jill R. Presser*, pour l'intervenante Criminal Lawyers' Association of Ontario.

Version française du jugement de la Cour rendu par

LE JUGE CROMWELL —

I. Introduction

[1] L'existence d'Internet remet en question la protection de la vie privée et soulève une multitude de questions inédites et épineuses à cet égard. Le présent pourvoi porte sur une de ces questions.

[2] La police a découvert l'adresse de protocole Internet (IP) de l'ordinateur qu'une personne avait

using to access and store child pornography through an Internet file-sharing program. They then obtained from the Internet Service Provider (ISP), without prior judicial authorization, the subscriber information associated with that IP address. This led them to the appellant, Mr. Spencer. He had downloaded child pornography into a folder that was accessible to other Internet users using the same file-sharing program. He was charged and convicted at trial of possession of child pornography and acquitted on a charge of making it available.

[3] At trial, Mr. Spencer claimed that the police had conducted an unconstitutional search by obtaining subscriber information matching the IP address and that the evidence obtained as a result should be excluded. He also testified that he did not know that others could have access to the shared folder and argued that he therefore did not knowingly make the material in the folder available to others. The trial judge concluded that there had been no breach of Mr. Spencer's right to be secure against unreasonable searches and seizures. However, he was of the view that the "making available" offence required some "positive facilitation" of access to the pornography, which Mr. Spencer had not done, and further he believed Mr. Spencer's evidence that he did not know that others could access his folder so that the fault element (*mens rea*) of the offence had not been proved. The judge therefore convicted Mr. Spencer of the possession offence, but acquitted him of the making available charge.

[4] The Court of Appeal upheld the conviction for possession of child pornography, agreeing with the trial judge that obtaining the subscriber information was not a search and holding that even if it were a search, it would have been reasonable. The court, however, set aside the acquittal on the making available charge on the basis that the trial judge had been wrong to require proof of positive facilitation

utilisé pour accéder à de la pornographie juvénile et pour la stocker à l'aide d'un programme de partage de fichiers. Les policiers ont ensuite obtenu auprès du fournisseur de services Internet (FSI), sans autorisation judiciaire préalable, les renseignements relatifs à l'abonnée à qui appartenait cette adresse IP. Ils ont ainsi découvert l'appelant, M. Spencer. Celui-ci avait téléchargé de la pornographie juvénile dans un répertoire qui était accessible à d'autres internautes utilisateurs du même programme de partage de fichiers. M. Spencer a été inculpé, puis, au procès, déclaré coupable de possession de pornographie juvénile et acquitté de l'infraction de rendre accessible de la pornographie juvénile.

[3] Au procès, M. Spencer a fait valoir que la police avait effectué une fouille ou une perquisition inconstitutionnelle lorsqu'elle a obtenu les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP et que la preuve ainsi obtenue devait être écartée. Il a également déclaré dans son témoignage qu'il ignorait que d'autres personnes pouvaient avoir accès au répertoire partagé et qu'il n'a donc pas sciemment rendu les fichiers accessibles. Le juge du procès a conclu qu'il n'y avait pas eu de violation du droit de M. Spencer à la protection contre les fouilles, les perquisitions et les saisies abusives. Il a toutefois estimé que pour être déclaré coupable de l'infraction de « rendre accessible » il faut avoir donné un certain [TRADUCTION] « appui délibéré » à l'accès à la pornographie, ce que M. Spencer n'avait pas fait. Il a également jugé que la déposition de M. Spencer selon laquelle il ignorait que d'autres personnes pouvaient avoir accès à son répertoire était véridique, de sorte que l'élément de faute de cette infraction (*mens rea*) n'avait pas été établi. Le juge a donc déclaré M. Spencer coupable de l'infraction de possession, mais l'a acquitté de l'accusation de rendre accessible.

[4] La Cour d'appel a confirmé la déclaration de culpabilité pour possession de pornographie juvénile, souscrivant à la conclusion du juge du procès selon laquelle le fait d'obtenir les renseignements relatifs à l'abonnée ne constituait pas une fouille ou une perquisition et concluant que, même s'il y en avait eu une, elle aurait été raisonnable. La cour a cependant annulé l'acquittement quant à l'accusation

of access by others to the material. A new trial was ordered on this charge.

[5] The appeal to this Court raises four issues which I would resolve as follows:

1. Did the police obtaining the subscriber information matching the IP address from the ISP constitute a search?

In my view, it did.

2. If so, was the search authorized by law?

In my view, it was not.

3. If not, should the evidence obtained as a result be excluded?

In my view, the evidence should not be excluded.

4. Did the trial judge err with respect to the fault element of the "making available" offence?

The judge did err and I would uphold the Court of Appeal's order for a new trial.

II. Analysis

A. *Did the Police Obtaining the Subscriber Information Matching the IP Address From the ISP Constitute a Search?*

[6] Mr. Spencer maintains that the police were conducting a search when they obtained the subscriber information associated with the IP address from the ISP, Shaw Communications Inc. The respondent Crown takes the opposite view. I agree with Mr. Spencer on this point. I will first set out a

de rendre accessible au motif que le juge du procès avait eu tort d'exiger la preuve d'un appui délibéré à l'accès aux fichiers par d'autres personnes et elle a ordonné la tenue d'un nouveau procès quant à ce chef d'accusation.

[5] Le présent pourvoi soulève quatre questions auxquelles je suis d'avis de répondre comme suit :

1. L'obtention par la police, auprès du FSI, des renseignements sur l'abonnée à qui appartenait l'adresse IP constitue-t-elle une fouille ou une perquisition?

Je suis d'avis que oui.

2. Si oui, la fouille ou la perquisition était-elle autorisée par la loi?

Je suis d'avis que non.

3. Sinon, la preuve ainsi obtenue devrait-elle être écartée?

J'estime que la preuve ne devrait pas être écartée.

4. Le juge du procès a-t-il commis une erreur relativement à l'élément de faute de l'infraction qui consiste à « rendre accessible »?

Le juge a effectivement commis une erreur et je suis d'avis de confirmer l'ordonnance de la Cour d'appel visant la tenue d'un nouveau procès.

II. Analyse

A. *L'obtention par la police, auprès du FSI, des renseignements sur l'abonnée à qui appartenait l'adresse IP constitue-t-elle une fouille ou une perquisition?*

[6] Monsieur Spencer soutient que la police effectuait une fouille ou une perquisition lorsqu'elle a obtenu, auprès du FSI, Shaw Communications Inc., les renseignements relatifs à l'abonnée à qui appartenait l'adresse IP en cause en l'espèce. Le ministère public intimé adopte le point de vue

summary of the relevant facts then turn to the legal analysis.

(1) Facts and Judicial History

[7] Mr. Spencer, who lived with his sister, connected to the Internet through an account registered in his sister's name. He used the file-sharing program LimeWire on his desktop computer to download child pornography from the Internet. LimeWire is a free peer-to-peer file-sharing program that, at the time, anyone could download onto their computer. Peer-to-peer systems such as LimeWire allow users to download files directly from the computers of other users. LimeWire does not have one central database of files, but instead relies on its users to share their files directly with others. It is commonly used to download music and movies and can also be used to download both adult and child pornography. It was Mr. Spencer's use of the file-sharing software that brought him to the attention of the police and which ultimately led to the search at issue in this case.

[8] Det. Sgt. Darren Parisien (then Cst.) of the Saskatoon Police Service, by using publicly available software, searched for anyone sharing child pornography. He could access whatever another user of the software had in his or her shared folder. In other words, he could "see" what other users of the file-sharing software could "see". He could also obtain two numbers related to a given user: the IP address that corresponds to the particular Internet connection through which a computer accesses the Internet at the time and the globally unique identifier (GUID) number assigned to each computer using particular software. The IP address of the computer from which shared material is obtained is displayed as part of the file-sharing process. There is little information in the record about the nature of IP addresses in general or the IP addresses provided

contraire. Je suis d'accord avec M. Spencer sur ce point. Je présenterai tout d'abord un résumé des faits pertinents; je procéderai ensuite à l'analyse juridique.

(1) Les faits et l'historique judiciaire

[7] Monsieur Spencer, qui habitait avec sa sœur, se connectait à Internet à partir d'un compte ouvert au nom de cette dernière. Il utilisait le programme de partage de fichiers LimeWire sur son ordinateur pour télécharger de la pornographie juvénile à partir d'Internet. LimeWire est un logiciel gratuit de partage de fichiers poste à poste que chacun pouvait télécharger à l'époque sur son ordinateur. Les systèmes poste à poste, comme LimeWire, permettent aux utilisateurs de télécharger des fichiers directement à partir des ordinateurs d'autres utilisateurs. LimeWire ne comporte pas de base de données centrale. Il compte plutôt sur ses utilisateurs qui partagent directement leurs fichiers avec d'autres utilisateurs. Le logiciel est couramment utilisé pour télécharger de la musique et des films, mais il peut aussi servir à télécharger de la pornographie tant adulte que juvénile. C'est l'utilisation du programme de partage de fichiers par M. Spencer qui a retenu l'attention de la police et qui a finalement mené à la fouille ou à la perquisition qui fait l'objet du présent litige.

[8] À l'aide d'un logiciel accessible au public, l'agent Darren Parisien (nommé sergent-détective depuis), du Service de police de Saskatoon, a recherché des personnes qui partageaient des fichiers de pornographie juvénile. Il pouvait accéder au contenu des répertoires partagés appartenant à d'autres utilisateurs du logiciel. Autrement dit, il pouvait [TRADUCTION] « voir » ce que d'autres utilisateurs du programme de partage de fichiers pouvaient « voir ». Il pouvait également obtenir deux numéros associés à un utilisateur donné : l'adresse IP correspondant à la connexion Internet établie par un ordinateur et l'identificateur global unique (GUID), soit le numéro associé à chaque ordinateur qui utilise un logiciel donné. L'adresse IP de l'ordinateur à partir duquel on obtient des fichiers partagés est affichée dans le cadre du processus de partage de

by Shaw to its subscribers. There is a description in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at paras. 21-26, which also notes some of the differences that may exist among IP addresses. For the purposes of this case, what we know is that the IP address obtained by Det. Sgt. Parisien matched computer activity at the particular point in time that he was observing that activity.

[9] Det. Sgt. Parisien generated a list of IP addresses for computers that had shared what he believed to be child pornography. He then ran that list of IP addresses against a database which matches IP addresses with approximate locations. He found that one of the IP addresses was suspected to be in Saskatoon, with Shaw as the ISP.

[10] Det. Sgt. Parisien then determined that Mr. Spencer's computer was online and connected to LimeWire. As a result, he (along with any LimeWire user) was able to browse the shared folder. He saw an extensive amount of what he believed to be child pornography. What he lacked was knowledge of where exactly the computer was and who was using it.

[11] To connect the computer usage to a location and potentially a person, investigators made a written "law enforcement request" to Shaw for the subscriber information including the name, address and telephone number of the customer using that IP address. The request, which was purportedly made pursuant to s. 7(3)(*c.*1)(ii) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*), indicated that police were investigating an offence under the *Criminal Code*, R.S.C. 1985, c. C-46, pertaining to child pornography and the Internet and that the subscriber information was being sought as part of an ongoing investigation. (The full text of the relevant statutory provisions is set out in an Appendix.) Investigators

fichiers. Il y a peu de renseignements au dossier sur la nature des adresses IP en général ou des adresses IP que Shaw fournit à ses abonnés. Dans l'arrêt *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, par. 21-26, on trouve une description de certaines des différences qui existent entre les adresses IP. Pour les besoins de l'espèce, une chose est certaine : l'adresse IP qu'a obtenue le sergent-détective Parisien correspondait aux activités informatiques qui se déroulaient au moment précis où il les observait.

[9] Le sergent-détective Parisien a dressé une liste des adresses IP correspondant aux ordinateurs qui avaient été utilisés pour le partage de ce qu'il estimait être de la pornographie juvénile. Il a ensuite comparé cette liste aux renseignements figurant dans une base de données qui permet d'associer des adresses IP à des emplacements approximatifs. Il a découvert qu'une des adresses IP semblait se trouver à Saskatoon et que Shaw était le FSI.

[10] Le sergent-détective Parisien a ensuite déterminé que l'ordinateur de M. Spencer était connecté à Internet ainsi qu'à LimeWire. Par conséquent, le sergent-détective (ainsi que tout autre utilisateur du logiciel LimeWire) pouvait parcourir le répertoire partagé du suspect. Il a vu une grande quantité de ce qu'il estimait être de la pornographie juvénile. Il ne connaissait cependant pas l'emplacement exact de l'ordinateur ni l'identité de son utilisateur.

[11] Pour établir un lien entre les activités informatiques en question et un emplacement précis, et potentiellement une personne, les enquêteurs ont présenté par écrit à Shaw une [TRADUCTION] « demande de la part des autorités d'application de la loi » en vue d'obtenir des renseignements relatifs à l'abonnée qui utilisait cette adresse IP, soit, notamment, son nom, son adresse et son numéro de téléphone. La demande — qui aurait été fondée sur le sous-al. 7(3)*c.*1)(ii) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (*LPRPDE*) — indiquait que la police enquêtait sur une infraction prévue au *Code criminel*, L.R.C. 1985, ch. C-46, relative à la pornographie juvénile et à Internet et

did not have or try to obtain a production order (i.e. the equivalent of a search warrant in this context).

[12] Shaw complied with the request and provided the name, address and telephone number of the customer associated with the IP address, Mr. Spencer's sister. With this information in hand, the police obtained a warrant to search Ms. Spencer's home (where Mr. Spencer lived) and seize his computer, which they did. The search of Mr. Spencer's computer revealed about 50 child pornography images and two child pornography videos.

[13] Mr. Spencer was charged with possessing child pornography contrary to s. 163.1(4) of the *Criminal Code* and making child pornography available over the Internet contrary to s. 163.1(3). There is no dispute that the images found in his shared folder were child pornography.

[14] At trial, Mr. Spencer sought to exclude the evidence found on his computer on the basis that the police actions in obtaining his address from Shaw without prior judicial authorization amounted to an unreasonable search contrary to s. 8 of the *Canadian Charter of Rights and Freedoms*. The trial judge rejected this contention and convicted Mr. Spencer of the possession count. On appeal, the Saskatchewan Court of Appeal upheld the judge's decision with respect to the search issue.

(2) Was the Request to Shaw a Search?

[15] Under s. 8 of the *Charter*, "[e]veryone has the right to be secure against unreasonable search or seizure." This Court has long emphasized the need

que les renseignements relatifs à l'abonnée étaient demandés aux fins d'une enquête qui était en cours. (Les dispositions législatives pertinentes sont reproduites en annexe.) Les enquêteurs n'avaient pas obtenu ni tenté d'obtenir une ordonnance de communication (c.-à-d. l'équivalent d'un mandat de perquisition dans ce contexte).

[12] Shaw a donné suite à la demande et a fourni le nom, l'adresse et le numéro de téléphone de la sœur de M. Spencer, la cliente à qui appartenait l'adresse IP. À l'aide de ces renseignements, la police a obtenu un mandat permettant de perquisitionner dans la résidence de M^me^ Spencer, où habitait M. Spencer, et de saisir l'ordinateur de celui-ci, ce que les policiers ont fait. La fouille de l'ordinateur de M. Spencer a permis de découvrir environ 50 images et deux vidéos de pornographie juvénile.

[13] Monsieur Spencer a été accusé de possession de pornographie juvénile, infraction décrite au par. 163.1(4) du *Code criminel*, et de rendre accessible de la pornographie juvénile sur Internet, en contravention du par. 163.1(3). Le fait que les images trouvées dans son répertoire partagé constituaient de la pornographie juvénile n'est pas contesté.

[14] Au procès, M. Spencer a tenté de faire écarter les éléments de preuve découverts sur son ordinateur au motif que les mesures prises sans autorisation judiciaire préalable par les policiers, en vue d'obtenir son adresse auprès de Shaw, correspondaient à une fouille ou à une perquisition abusive et contrevenaient à l'art. 8 de la *Charte canadienne des droits et libertés*. Le juge du procès a rejeté cette prétention et déclaré M. Spencer coupable de l'infraction de possession. La Cour d'appel de la Saskatchewan a confirmé la décision du juge relativement à la question de la fouille ou de la perquisition.

(2) La demande adressée à Shaw constituait-elle une fouille ou une perquisition?

[15] Suivant l'article 8 de la *Charte*, « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. » La Cour insiste

for a purposive approach to s. 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 156-57; *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 427-28; *R. v. Plant*, [1993] 3 S.C.R. 281, at pp. 292-93; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paras. 12-16; *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, [2013] 3 S.C.R. 733, at para. 22.

depuis longtemps sur la nécessité d'adopter, à l'égard de l'art. 8, une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère : *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 156-157; *R. c. Dyment*, [1988] 2 R.C.S. 417, p. 427-428; *R. c. Plant*, [1993] 3 R.C.S. 281, p. 292-293; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, par. 12-16; *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733, par. 22.

[16] The first issue is whether this protection against unreasonable searches and seizures was engaged here. That depends on whether what the police did to obtain the subscriber information matching the IP address was a search or seizure within the meaning of s. 8 of the *Charter*. The answer to this question turns on whether, in the totality of the circumstances, Mr. Spencer had a reasonable expectation of privacy in the information provided to the police by Shaw. If he did, then obtaining that information was a search.

[16] En premier lieu, il s'agit de savoir si cette protection contre les fouilles, les perquisitions et les saisies abusives s'applique en l'espèce. Pour le savoir, il faut déterminer si les mesures prises par la police en vue d'obtenir les renseignements sur l'abonnée à qui appartenait l'adresse IP constituaient une fouille, une perquisition ou une saisie au sens de l'art. 8 de la *Charte*. Pour ce faire, il faut déterminer si, compte tenu de l'ensemble des circonstances, M. Spencer s'attendait raisonnablement au respect du caractère privé des renseignements fournis par Shaw à la police. Si tel était le cas, l'obtention de ces renseignements constituait une fouille ou une perquisition.

[17] We assess whether there is a reasonable expectation of privacy in the totality of the circumstances by considering and weighing a large number of interrelated factors. These include both factors related to the nature of the privacy interests implicated by the state action and factors more directly concerned with the expectation of privacy, both subjectively and objectively viewed, in relation to those interests: see, e.g., *Tessling*, at para. 38; *Ward*, at para. 65. The fact that these considerations must be looked at in the "totality of the circumstances" underlines the point that they are often interrelated, that they must be adapted to the circumstances of the particular case and that they must be looked at as a whole.

[17] On détermine s'il existe une attente raisonnable en matière de respect de la vie privée, compte tenu de l'ensemble des circonstances, en examinant et en soupesant un grand nombre de facteurs interreliés qui comprennent à la fois des facteurs relatifs à la nature des droits en matière de vie privée visés par l'action de l'État et des facteurs qui ont trait plus directement à l'attente en matière de respect de la vie privée, considérée tant subjectivement qu'objectivement, par rapport à ces droits : voir, p. ex., *Tessling*, par. 38; *Ward*, par. 65. La nécessité d'examiner ces éléments compte tenu de « l'ensemble des circonstances » fait ressortir le fait qu'ils sont souvent interdépendants, qu'ils doivent être adaptés aux circonstances de chaque cas, et qu'ils doivent être considérés dans leur ensemble.

[18] The wide variety and number of factors that may be considered in assessing the reasonable expectation of privacy can be grouped under four main headings for analytical convenience: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: *Tessling*, at para. 32; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 27; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 40. However, this is not a purely factual inquiry. The reasonable expectation of privacy standard is normative rather than simply descriptive: *Tessling*, at para. 42. Thus, while the analysis is sensitive to the factual context, it is inevitably "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy": *Patrick*, at para. 14; see also *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, and *Ward*, at paras. 81-85.

[19] I can deal quite briefly with two aspects of the appeal. The trial judge in this case held that there was no subjective expectation of privacy in this case: 2009 SKQB 341, 361 Sask. R. 1, at para. 18. However, as I will explain below, the trial judge reached this conclusion by incorrectly defining the subject matter of the search. On the proper understanding of the scope of the search, Mr. Spencer's subjective expectation of privacy in his online activities can readily be inferred from his use of the network connection to transmit sensitive information: *Cole*, at para. 43. Mr. Spencer's direct interest in the subject matter of the search is equally clear. Though he was not personally a party to the contract with the ISP, he had access to the Internet with the permission of the subscriber and his use of the Internet was by means of his own computer in his own place of residence.

[18] La grande variété et le nombre important de facteurs pouvant être pris en considération pour évaluer les attentes raisonnables en matière de respect de la vie privée peuvent être regroupés, par souci de commodité, en quatre grandes catégories : (1) l'objet de la fouille ou de la perquisition contestée; (2) le droit du demandeur à l'égard de l'objet; (3) l'attente subjective du demandeur en matière de respect de sa vie privée relativement à l'objet; et (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances : *Tessling*, par. 32; *R. c. Patrick*, 2009 CSC 17, [2009] 1 R.C.S. 579, par. 27; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 40. Il ne s'agit toutefois pas d'un examen purement factuel. L'attente raisonnable en matière de vie privée est de nature normative et non simplement descriptive : *Tessling*, par. 42. Ainsi, même si l'analyse du droit au respect de la vie privée tient compte du contexte factuel, elle « abonde [inévitablement] en jugements de valeur énoncés du point de vue indépendant de la personne raisonnable et bien informée, qui se soucie des conséquences à long terme des actions gouvernementales sur la protection du droit au respect de la vie privée privée » : *Patrick*, par. 14; voir aussi *R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211, par. 34, et *Ward*, par. 81-85.

[19] Quelques brefs commentaires suffiront pour traiter deux aspects du pourvoi. Selon le juge du procès, il n'y avait pas d'attente subjective en matière de vie privée dans la présente affaire : 2009 SKQB 341, 361 Sask. R. 1, par. 18. Toutefois, comme je vais l'expliquer ultérieurement, la conclusion du juge du procès reposait sur une définition inexacte de l'objet de la fouille ou de la perquisition. Selon une interprétation juste de cet objet, l'attente subjective de M. Spencer au respect du caractère privé de ses activités en ligne peut aisément être déduite de son utilisation de la connexion réseau pour transmettre des renseignements sensibles : *Cole*, par. 43. L'intérêt direct de M. Spencer à l'égard de l'objet de la fouille ou de la perquisition est également manifeste. Même s'il n'était pas personnellement parti au contrat conclu avec le FSI, il avait accès à Internet avec la permission de l'abonnée et il l'utilisait au moyen de son propre ordinateur, à son lieu de résidence.

[20] The main dispute in this case thus turns on the subject matter of the search and whether Mr. Spencer's subjective expectation of privacy was reasonable. The two circumstances relevant to determining the reasonableness of his expectation of privacy in this case are the nature of the privacy interest at stake and the statutory and contractual framework governing the ISP's disclosure of subscriber information.

[21] In this case, I have found it helpful to look first at the subject matter of the search, then at the nature of the privacy interests implicated by the state actions and then finally at the governing contractual and statutory framework. While these subjects are obviously interrelated, approaching the analysis under these broad headings provides a degree of focus while permitting full examination of the "totality of the circumstances".

(a) *The Subject Matter of the Search*

[22] Mr. Spencer alleges that the police request to Shaw is a state action that constitutes a search or seizure for the purposes of s. 8 of the *Charter*. We must therefore consider what the subject matter of that request was in order to be able to identify the privacy interests that were engaged by it.

[23] In many cases, defining the subject matter of the police action that is alleged to be a search is straightforward. In others, however, it is not. This case falls into the latter category. The parties and the courts below have markedly divergent perspectives on this important issue, a divergence which is reflected in the jurisprudence: see, for example, the authorities reviewed in *Ward*, at para. 3.

[24] Mr. Spencer contends that the subject matter of the alleged search was core biographical data, revealing intimate and private information about the people living at the address provided by Shaw which matched the IP address. The Crown, on the

[20] Dans la présente affaire, le litige porte donc principalement sur l'objet de la fouille ou de la perquisition et sur la question de savoir si l'attente subjective de M. Spencer en matière de vie privée était raisonnable. Les deux éléments pertinents pour déterminer le caractère raisonnable de son attente au respect de sa vie privée sont, d'une part, la nature de l'intérêt en matière de vie privée qui est en jeu et, d'autre part, le cadre législatif et contractuel régissant la communication par le FSI des renseignements relatifs à l'abonnée.

[21] En l'espèce, j'ai jugé utile d'examiner d'abord l'objet de la fouille ou de la perquisition, ensuite la nature des droits en matière de vie privée que mettent en jeu les actes de l'État et, enfin, le cadre législatif et contractuel applicable. Il s'agit manifestement d'éléments interreliés, mais l'analyse axée sur ces vastes catégories assure une certaine précision tout en permettant d'examiner de manière exhaustive « l'ensemble des circonstances ».

a) *L'objet de la fouille ou de la perquisition*

[22] Selon M. Spencer, c'est la demande faite à Shaw par la police qui constitue l'action de l'État correspondant à une fouille, à une perquisition ou à une saisie aux fins de l'application de l'art. 8 de la *Charte*. Nous devons donc examiner l'objet de cette demande pour pouvoir déterminer quels étaient les droits en jeu en matière de vie privée.

[23] Dans bien des cas, il est facile de définir l'objet de l'action de la police qui, selon les allégations, constitue une fouille ou une perquisition. Ce n'est par contre pas toujours ainsi; et la présente espèce appartient à cette seconde catégorie. Les parties et les tribunaux de juridiction inférieure ont adopté des positions nettement divergentes sur cette question importante, situation qui se retrouve également dans la jurisprudence : voir, par exemple, les décisions mentionnées dans l'arrêt *Ward*, par. 3.

[24] Monsieur Spencer fait valoir que l'objet de la fouille ou de la perquisition contestée comportait des renseignements d'ordre biographique, soit des renseignements personnels et confidentiels sur les personnes habitant à l'adresse fournie par Shaw

other hand, maintains that the subject matter of the alleged search was simply a name, address and telephone number matching a publicly available IP address.

[25] These divergent views were reflected in the decisions of the Saskatchewan courts. The trial judge adopted the Crown's view that what the police sought and obtained was simply generic information that does not touch on the core of Mr. Spencer's biographical information. Ottenbreit J.A. in the Court of Appeal was of largely the same view. For him, the information sought by the police in this case simply established the identity of the contractual user of the IP address. The fact that this information might eventually reveal a good deal about the activity of identifiable individuals on the Internet was, for him, "neither here nor there": 2011 SKCA 144, 377 Sask. R. 280, at para. 110 (see also *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, at paras. 119-24 and 134). In contrast to this approach, Caldwell J.A. (Cameron J.A. concurring on this point) held that in characterizing the subject matter of the alleged search, it is important to look beyond the "mundane" subscriber information such as name and address (para. 22). The potential of that information to reveal intimate details of the lifestyle and personal choices of the individual must also be considered: see also *Trapp*, *per* Cameron J.A., at paras. 33-37.

[26] I am in substantial agreement with Caldwell and Cameron JJ.A. on this point. While, in many cases, defining the subject matter of the search will be uncontroversial, in cases in which it is more difficult, the Court has taken a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake. The Court has looked at not only the nature of the precise information sought, but also at the nature of the information that it reveals.

qui correspondait à l'adresse IP. Pour sa part, le ministère public soutient que la fouille ou la perquisition contestée visait plutôt simplement le nom, l'adresse et le numéro de téléphone correspondant à une adresse IP accessible au public.

[25] Les tribunaux de la Saskatchewan ont exprimé les mêmes opinions divergentes. Le juge du procès a adopté le point de vue du ministère public selon lequel la police n'avait recherché et obtenu que des renseignements d'ordre général qui ne correspondent pas à des données d'ordre biographique relatives à M. Spencer. Le juge Ottenbreit de la Cour d'appel a partagé en grande partie la même opinion. À son avis, les renseignements recherchés par la police en l'espèce ne faisaient qu'établir l'identité de l'utilisateur de l'adresse IP qui était désigné dans le contrat. La possibilité que ces renseignements finissent par révéler plusieurs aspects des activités menées par des personnes identifiables sur Internet était [TRADUCTION] « sans importance » : 2011 SKCA 144, 377 Sask. R. 280, par. 110 (voir également *R. c. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, par. 119-124 et 134). Par contre, selon le juge Caldwell (le juge Cameron a souscrit à son opinion à ce sujet), lorsqu'il s'agit de qualifier l'objet d'une fouille ou d'une perquisition contestée, il faut aller au-delà des renseignements [TRADUCTION] « banals » relatifs à l'abonné, tels son nom et son adresse (par. 22). Il faut aussi tenir compte de la possibilité que ces renseignements révèlent des détails intimes sur le mode de vie et les choix personnels de l'individu : voir également l'arrêt *Trapp*, le juge Cameron, par. 33-37.

[26] Je souscris pour l'essentiel aux conclusions formulées sur ce point par les juges Caldwell et Cameron de la Cour d'appel. Dans bien des cas, la définition de l'objet de la fouille ou de la perquisition fait l'unanimité. Cependant, dans les cas qui posent davantage de difficultés à cet égard, la Cour a adopté dans le passé une approche large et fonctionnelle, en examinant le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui est en jeu. La Cour a examiné non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés.

[27] A number of decisions of the Court reflect this approach. I begin with *Plant*. There, the Court, dealing with informational privacy, stressed the strong claim to privacy in relation to information that is at the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state": p. 293. Importantly, the Court went on to make clear that s. 8 protection is accorded not only to the information which is itself of that nature, but also to "information which tends to reveal intimate details of the lifestyle and personal choices of the individual": *ibid.* (emphasis added).

[28] *Tessling* took the same approach, although it led to a different conclusion. The subject matter of the alleged search was held to be the heat emitted from the surface of a building. The Forward Looking Infra-Red (FLIR) imaging technique was used to help assess the activities that transpired inside a house, but the heat emissions by themselves could not distinguish between one heat source and another. In short, the heat emanations were, on their own, meaningless because they did not permit any inferences about the precise activity giving rise to the heat: paras. 35-36. The critical question was: what inferences about activity inside the home — admittedly a highly private zone — did the FLIR images support?

[29] I turn next to *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456, and the companion appeal in *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569. While the Court divided on other points, it was unanimous in holding that the dog sniff of Mr. Kang-Brown's bag constituted a search. As explained by both Deschamps and Bastarache JJ., the dog sniffing at the air in the vicinity of the bag functioned as an investigative procedure that allowed for a "strong, immediate and direct inference" about what was or was not inside the bag: Deschamps J., at paras. 174-75; Bastarache J., at para. 227. Thus, while the "information" obtained by the sniffer dog was simply the smell of the air outside the bag, the dog's

[27] Plusieurs arrêts de la Cour reflètent cette approche. J'examinerai d'abord l'arrêt *Plant*. Dans cette affaire concernant des aspects informationnels de la vie privée, la Cour a insisté sur le droit garanti au respect de la vie privée relativement à des renseignements « biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État » : p. 293. Fait important, la Cour a ensuite précisé que la protection garantie par l'art. 8 vise non seulement les renseignements de cette nature, mais aussi les « renseignements tendant à révéler des détails intimes sur le mode de vie et les choix personnels de l'individu » : *ibid.* (je souligne).

[28] La Cour a suivi la même approche dans l'arrêt *Tessling*, mais elle a tiré une conclusion différente. Dans cette affaire, il a été conclu que l'objet de la perquisition contestée était la chaleur émanant de la surface d'un édifice. La technique d'imagerie FLIR (système infrarouge à vision frontale) a servi à évaluer les activités qu'il y avait à l'intérieur d'une résidence, mais les émanations de chaleur ne permettaient pas, à elles seules, de distinguer les sources de chaleur. Bref, les émanations de chaleur n'avaient, en elles-mêmes, aucune signification, parce qu'elles ne permettaient pas de déduire quelle activité précise produisait la chaleur : par. 35-36. La question cruciale portait sur la nature des activités que permettaient de déduire les images FLIR et qui se déroulaient à l'intérieur de la résidence — nous en conviendrons, un lieu de nature éminemment privée.

[29] Je passe maintenant à l'arrêt *R. c. Kang-Brown*, 2008 CSC 18, [2008] 1 R.C.S. 456, et au pourvoi connexe *R. c. A.M.*, 2008 CSC 19, [2008] 1 R.C.S. 569. La Cour était divisée sur d'autres points, mais elle a conclu à l'unanimité que la vérification du sac de M. Kang-Brown à l'aide d'un chien renifleur constituait une fouille. Comme l'ont expliqué les juges Deschamps et Bastarache, en décelant ce qu'il y avait dans l'air à proximité du sac, le chien a servi d'outil d'enquête et son intervention a « immédiatement et directement permis [aux policiers] de faire une forte inférence » quant au contenu du sac : la juge Deschamps, par. 174-175; le juge Bastarache, par. 227. Ainsi,

reaction to it provided the police with a strong inference as to what was inside. As Binnie J. put it in *A.M.* (which concerned a dog sniff of the accused's backpack), "[b]y use of the dog, the policeman could 'see' through the concealing fabric of the backpack": para. 67.

[30] How to characterize the subject matter of an alleged search was addressed by the Court most recently in *Gomboc*. While the Court was divided on other matters, it was unanimous about the framework that must be applied in considering the subject matter of a "search". The Court considered the strength of the inference between data derived from a digital recording ammeter (DRA) and particular activities going on in a residence in assessing whether use of the DRA constituted a search. Abella J. (Binnie and LeBel JJ. concurring) took into account "the strong and reliable inference that can be made from the patterns of electricity consumption . . . as to the presence within the home of one particular activity": para. 81 (emphasis added). The Chief Justice and Fish J. referred to the fact that the DRA data "sheds light on private activities within the home": para. 119. Deschamps J. (Charron, Rothstein and Cromwell JJ. concurring) spoke in terms of the extent to which the DRA data was revealing of activities in the home: para. 38.

[31] Thus, it is clear that the tendency of information sought to support inferences in relation to other personal information must be taken into account in characterizing the subject matter of the search. The correct approach was neatly summarized by Doherty J.A. in *Ward*, at para. 65. When identifying the subject matter of an alleged search, the court must not do so "narrowly in terms of the physical acts involved or the physical space invaded,

bien que les « informations » recueillies par le chien renifleur tenaient simplement de l'odeur qu'il y avait dans l'air à l'extérieur du sac, la réaction du chien a permis aux policiers de faire une forte inférence quant au contenu du sac. Comme l'a indiqué le juge Binnie dans l'arrêt *A.M.* (qui portait sur l'intervention d'un chien renifleur pour vérifier le sac à dos de l'accusé), « [e]n se servant du chien, le policier a pu "voir" à travers le tissu opaque du sac à dos » : par. 67.

[30] La façon de définir l'objet d'une fouille ou d'une perquisition contestée a été examinée pour la dernière fois par la Cour dans l'arrêt *Gomboc*. Bien qu'elle fût divisée sur d'autres questions, elle s'est prononcée à l'unanimité sur le cadre d'analyse à appliquer pour déterminer l'objet d'une « fouille ou [d'une] perquisition ». Dans cette affaire, la Cour a examiné la fiabilité des inférences qu'il est possible de tirer à partir des données enregistrées à l'aide d'un ampèremètre numérique muni d'un enregistreur (AN) au sujet d'activités données se déroulant à l'intérieur d'une résidence pour déterminer si l'utilisation de l'ampèremètre constituait une fouille ou une perquisition. La juge Abella (avec l'accord des juges Binnie et LeBel) a tenu compte « de la solidité et de la fiabilité des inférences pouvant être tirées à partir des cycles de consommation d'électricité [. . .] relativement à la tenue d'une activité particulière à une adresse » : par. 81 (je souligne). La Juge en chef et le juge Fish ont affirmé que les données enregistrées par l'AN « éclairent sur les activités privées se déroulant à l'intérieur de la maison » : par. 119. La juge Deschamps (avec l'accord des juges Charron, Rothstein et Cromwell) s'est demandé dans quelle mesure les données enregistrées par l'AN révèlent les activités qui se déroulent à l'intérieur de la maison : par. 38.

[31] Ainsi, il est évident que, pour définir l'objet de la fouille ou de la perquisition, il faut tenir compte de la tendance qui consiste à chercher à obtenir des renseignements pour permettre d'en tirer des inférences au sujet d'autres renseignements qui, eux, sont de nature personnelle. La méthode qu'il convient d'adopter a été clairement résumée par le juge Doherty au par. 65 de l'arrêt *Ward*. Lorsqu'elle est appelée à identifier l'objet

but rather by reference to the nature of the privacy interests potentially compromised by the state action": *ibid.*

[32] Applying this approach to the case at hand, I substantially agree with the conclusion reached by Cameron J.A. in *Trapp* and adopted by Caldwell J.A. in this case. The subject matter of the search was not simply a name and address of someone in a contractual relationship with Shaw. Rather, it was the identity of an Internet subscriber which corresponded to particular Internet usage. As Cameron J.A. put it, at para. 35 of *Trapp*:

> To label information of this kind as mere "subscriber information" or "customer information", or nothing but "name, address, and telephone number information", tends to obscure its true nature. I say this because these characterizations gloss over the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual, including the individual's online activity in the home.

[33] Here, the subject matter of the search is the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity.

(b) *Nature of the Privacy Interest Potentially Compromised by the State Action*

[34] The nature of the privacy interest engaged by the state conduct is another facet of the totality of the circumstances and an important factor in assessing the reasonableness of an expectation of privacy. The Court has previously emphasized an understanding of informational privacy as confidentiality and control of the use of intimate information about oneself. In my view, a somewhat

d'une fouille ou d'une perquisition contestée, une cour ne doit pas adopter une approche [TRADUCTION] « restrictive qui porte sur les actions commises ou sur l'espace envahi, mais plutôt une approche fondée sur la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte » : *ibid.*

[32] Si on applique cette méthode en l'espèce, je souscris pour l'essentiel à la conclusion tirée par le juge Cameron dans l'arrêt *Trapp* et adoptée par le juge Caldwell de la Cour d'appel dans la présente affaire. La fouille n'avait pas simplement pour objet le nom et l'adresse d'une personne qui était liée par contrat à Shaw. Il s'agissait plutôt de l'identité d'une abonnée aux services Internet à qui correspondait une utilisation particulière de ces services. Comme l'a affirmé le juge Cameron au par. 35 de l'arrêt *Trapp* :

> [TRADUCTION] Qualifier de tels renseignements de simples « renseignements relatifs à l'abonné » ou de « renseignements sur le client » ou encore de rien d'autre que de « renseignements sur le nom, l'adresse et le numéro de téléphone » tend à occulter leur véritable nature. Je tiens à le préciser, parce que ces qualifications font abstraction de l'importance d'une adresse IP et des renseignements que cette adresse, une fois liée à une personne en particulier, peut révéler sur cette personne, notamment les activités en ligne que celle-ci pratique dans sa résidence.

[33] En l'espèce, la fouille avait pour objet l'identité de l'abonnée dont la connexion à Internet correspondait à une activité informatique particulière sous surveillance.

b) *La nature de l'intérêt en matière de vie privée auquel l'action de l'État pourrait porter atteinte*

[34] La nature de l'intérêt en matière de vie privée visé par l'action de l'État constitue un autre aspect de l'ensemble des circonstances et un facteur important pour apprécier le caractère raisonnable d'une attente en matière de vie privée. Dans le passé, la Cour a souligné l'importance, lorsqu'il est question de renseignements personnels, d'interpréter le droit à la vie privée de telle sorte qu'il

broader understanding of the privacy interest at stake in this case is required to account for the role that anonymity plays in protecting privacy interests online.

[35] Privacy is admittedly a "broad and somewhat evanescent concept": *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at para. 67. Scholars have noted the theoretical disarray of the subject and the lack of consensus apparent about its nature and limits: see, e.g., C. D. L. Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011), 37 *Queen's L.J.* 167, at pp. 176-77. Notwithstanding these challenges, the Court has described three broad types of privacy interests — territorial, personal, and informational — which, while often overlapping, have proved helpful in identifying the nature of the privacy interest or interests at stake in particular situations: see, e.g., *Dyment*, at pp. 428-29; *Tessling*, at paras. 21-24. These broad descriptions of types of privacy interests are analytical tools, not strict or mutually-exclusive categories.

[36] The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought. To paraphrase Binnie J. in *Patrick*, the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography, but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes: *Patrick*, at para. 32.

protège tant la confidentialité que le contrôle des renseignements en question. À mon avis, il est nécessaire en l'espèce d'élargir quelque peu cette interprétation de manière à tenir compte du rôle que joue l'anonymat dans la protection des droits en matière de vie privée sur Internet.

[35] Certes, la vie privée est « une notion générale quelque peu évanescente » : *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403, par. 67. Certains auteurs ont souligné la confusion à ce sujet, sur le plan théorique, et l'absence de consensus apparent quant à ses nature et limites : voir, p. ex., C. D. L. Hunt, « Conceptualizing Privacy and Elucidating its Importance : Foundational Considerations for the Development of Canada's Fledgling Privacy Tort » (2011), 37 *Queen's L.J.* 167, p. 176-177. Nonobstant ces enjeux, la Cour a décrit trois grandes catégories de droits en matière de vie privée, qui regroupent notamment les aspects qui ont trait aux lieux, à la personne et à l'information, et qui, malgré leur chevauchement fréquent, ont permis de préciser la nature des droits en matière de vie privée en jeu dans des situations particulières : voir, p. ex., *Dyment*, p. 428-429; *Tessling*, par. 21-24. Il s'agit d'outils d'analyse, et non de catégories strictes ou mutuellement exclusives.

[36] La nature de l'intérêt en matière de vie privée ne dépend pas de la question de savoir si, dans un cas particulier, le droit à la vie privée masque une activité légale ou une activité illégale. En effet, l'analyse porte sur le caractère privé du lieu ou de l'objet visé par la fouille ou la perquisition ainsi que sur les conséquences de cette dernière pour la personne qui en fait l'objet, et non sur la nature légale ou illégale de la chose recherchée. Pour reprendre les propos du juge Binnie dans l'arrêt *Patrick*, il ne s'agit pas de savoir si l'appelant possédait un droit légitime au respect de la vie privée à l'égard de la dissimulation de son utilisation d'Internet dans le but d'accéder à de la pornographie juvénile, mais plutôt de savoir si, d'une manière générale, les citoyens ont droit au respect de leur vie privée à l'égard des renseignements concernant les abonnés de services Internet relativement aux ordinateurs qu'ils utilisent dans leur domicile à des fins privées : *Patrick*, par. 32.

[37] We are concerned here primarily with informational privacy. In addition, because the computer identified and in a sense monitored by the police was in Mr. Spencer's residence, there is an element of territorial privacy in issue as well. However, in this context, the location where the activity occurs is secondary to the nature of the activity itself. Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via smartphones, or portable devices. Therefore, here as in *Patrick*, at para. 45, the fact that a home was involved is not a controlling factor but is nonetheless part of the totality of the circumstances: see, e.g., *Ward*, at para. 90.

[38] To return to informational privacy, it seems to me that privacy in relation to information includes at least three conceptually distinct although overlapping understandings of what privacy is. These are privacy as secrecy, privacy as control and privacy as anonymity.

[39] Informational privacy is often equated with secrecy or confidentiality. For example, a patient has a reasonable expectation that his or her medical information will be held in trust and confidence by the patient's physician: see, e.g., *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, at p. 149.

[40] Privacy also includes the related but wider notion of control over, access to and use of information, that is, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others": A. F. Westin, *Privacy and Freedom* (1970), at p. 7, cited in *Tessling*, at para. 23. La Forest J. made this point in *Dyment*. The understanding of informational privacy as control "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" (*Dyment*, at p. 429, quoting from *Privacy and Computers*, the Report of the Task Force established by the Department of

[37] En l'espèce, nous nous intéressons principalement au caractère privé des renseignements personnels. En outre, puisque l'ordinateur repéré et, en quelque sorte, surveillé par la police se trouvait dans la résidence de M. Spencer, un aspect du droit à la vie privée lié aux lieux est aussi en jeu. Dans le présent contexte, le lieu de l'activité est toutefois accessoire à la nature de l'activité elle-même. En effet, les internautes ne s'attendent pas à perdre leur anonymat en ligne lorsqu'ils accèdent à Internet ailleurs que chez eux au moyen d'un téléphone intelligent ou d'un appareil portatif. En l'espèce, tout comme dans l'arrêt *Patrick*, par. 45, le fait qu'une résidence soit en cause ne constitue donc pas un facteur déterminant, mais fait néanmoins partie de l'ensemble des circonstances : voir, p. ex., *Ward*, par. 90.

[38] Pour revenir à la question du droit à la vie privée en ce qui a trait aux renseignements personnels, j'estime qu'il englobe au moins trois facettes qui se chevauchent, mais qui se distinguent sur le plan conceptuel. Il s'agit de la confidentialité, du contrôle et de l'anonymat.

[39] Le caractère privé des renseignements personnels est souvent assimilé à la confidentialité. Par exemple, le patient s'attend raisonnablement à ce que ses renseignements d'ordre médical demeurent confidentiels : voir, p. ex., *McInerney c. MacDonald*, [1992] 2 R.C.S. 138, p. 149.

[40] Or, le droit à la vie privée comprend également la notion connexe, mais plus large, de contrôle sur l'accès à l'information et sur l'utilisation des renseignements, c'est-à-dire [TRADUCTION] « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes à quel moment les renseignements les concernant sont communiqués, de quelle manière et dans quelle mesure » : A. F. Westin, *Privacy and Freedom* (1970), p. 7, cité dans *Tessling*, par. 23. Le juge La Forest a d'ailleurs souligné ce point dans l'arrêt *Dyment* en affirmant que la facette du droit à la vie privée en ce qui a trait aux renseignements personnels qui porte sur le contrôle « découle du postulat selon lequel l'information de caractère

Communications/Department of Justice (1972), at p. 13). Even though the information will be communicated and cannot be thought of as secret or confidential, "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected" (pp. 429-30); see also *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 46.

[41] There is also a third conception of informational privacy that is particularly important in the context of Internet usage. This is the understanding of privacy as anonymity. In my view, the concept of privacy potentially protected by s. 8 must include this understanding of privacy.

[42] The notion of privacy as anonymity is not novel. It appears in a wide array of contexts ranging from anonymous surveys to the protection of police informant identities. A person responding to a survey readily agrees to provide what may well be highly personal information. A police informant provides information about the commission of a crime. The information itself is not private — it is communicated precisely so that it will be communicated to others. But the information is communicated on the basis that it will not be identified with the person providing it. Consider situations in which the police want to obtain the list of names that correspond to the identification numbers on individual survey results or in which the defence in a criminal case wants to obtain the identity of the informant who has provided information that has been disclosed to the defence. The privacy interest at stake in these examples is not simply the individual's name, but the link between the identified individual and the personal information provided anonymously. As the intervener the Canadian Civil Liberties Association urged in its submissions,

personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend » (*Dyment*, p. 429, citant *L'ordinateur et la vie privée*, le Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice (1972), p. 13). Même si les renseignements seront divulgués et qu'ils ne peuvent être considérés comme confidentiels, « les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués » (p. 429-430); voir également *R. c. Duarte*, [1990] 1 R.C.S. 30, p. 46.

[41] Il existe aussi une troisième conception de l'aspect informationnel du droit à la vie privée qui revêt une importance particulière dans le contexte de l'utilisation d'Internet. Il s'agit de l'anonymat. À mon avis, le droit à la vie privée que garantirait l'art. 8 doit inclure cette conception de la vie privée.

[42] L'élément « anonymat » de la vie privée n'est pas nouveau. Il est présent dans un large éventail de contextes allant de sondages anonymes à la protection de l'identité des indicateurs de police. La personne qui répond à un sondage accepte volontiers de fournir ce qui peut fort bien être des renseignements de nature très personnelle. L'indicateur de police fournit des renseignements sur la perpétration d'un crime. Les renseignements en tant que tel ne sont pas privés — leur communication vise expressément la divulgation à d'autres personnes. Cela dit, cette communication tient compte du fait que l'identité de la personne qui fournit les renseignements demeurera confidentielle. Prenons, par exemple, des cas où la police veut obtenir la liste des noms correspondant aux numéros d'identification relativement aux résultats d'un sondage ou des cas où la partie défenderesse dans une affaire criminelle veut obtenir l'identité de l'indicateur ayant fourni les renseignements qui lui ont été communiqués. L'intérêt en matière de vie privée qui est en jeu dans ces exemples ne vise pas uniquement le nom d'une personne, mais

"maintaining anonymity can be integral to ensuring privacy": factum, at para. 7.

[43] Westin identifies anonymity as one of the basic states of privacy. Anonymity permits individuals to act in public places but to preserve freedom from identification and surveillance: pp. 31-32; see A. Slane and L. M. Austin, "What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011), 57 *Crim. L.Q.* 486, at p. 501. The Court's decision in *R. v. Wise*, [1992] 1 S.C.R. 527, provides an example of privacy in a public place. The Court held that the ubiquitous monitoring of a vehicle's whereabouts on public highways amounted to a violation of the suspect's reasonable expectation of privacy. It could of course have been argued that the electronic device was simply a convenient way of keeping track of where the suspect was driving his car, something that he was doing in public for all to see. But the Court did not take that approach.

[44] La Forest J. (who, while dissenting on the issue of exclusion of the evidence under s. 24(2), concurred with respect to the existence of a reasonable expectation of privacy), explained that "[i]n a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape'": p. 558 (emphasis added), quoting M. Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" (1988), 39 *Syracuse L. Rev.* 647, at p. 706. The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a

aussi le lien entre la personne désignée et les renseignements personnels fournis de façon anonyme. Comme l'a fait valoir l'Association canadienne des libertés civiles, intervenante en l'espèce, dans ses observations, [TRADUCTION] « le maintien de l'anonymat peut être essentiel pour garantir la protection de la vie privée » : mémoire, par. 7.

[43] Le professeur Westin présente l'anonymat comme une des facettes fondamentales de la vie privée. Selon lui, il permet aux personnes d'avoir des activités publiques tout en préservant la confidentialité de leur identité et en se protégeant contre la surveillance : p. 31-32; voir A. Slane et L. M. Austin, « What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations » (2011), 57 *Crim. L.Q.* 486, p. 501. L'arrêt *R. c. Wise*, [1992] 1 R.C.S. 527, donne un exemple du droit à la vie privée dans un endroit public. Dans cette affaire, la Cour a statué que la surveillance omniprésente des déplacements d'un véhicule sur la voie publique déjouait les attentes raisonnables du suspect en matière de vie privée. On aurait évidemment pu affirmer que le dispositif électronique ne constituait qu'un moyen pratique de suivre les déplacements en voiture du suspect, qu'il faisait d'ailleurs à la vue de tous. Mais la Cour n'a pas adopté cette approche.

[44] Le juge La Forest (qui, bien que dissident sur la question de l'exclusion de la preuve en application du par. 24(2), a souscrit à l'existence d'une attente raisonnable en matière du respect de la vie privée), a expliqué que, « [s]'il est normal, dans divers contextes publics, d'être observé fortuitement, nous aurions par contre toutes les raisons d'être choqués par des regards insistants. Dans ces activités publiques, nous ne nous attendons pas à être identifiés personnellement et soumis à une surveillance intensive, mais nous cherchons plutôt à passer inaperçus » : p. 558 (je souligne), citant M. Gutterman, « A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance » (1988), 39 *Syracuse L. Rev.* 647, p. 706. Le simple fait qu'une personne quitte l'intimité de sa résidence et pénètre dans un lieu public ne signifie

person may not be able to control who observes him or her in public. Thus, in order to uphold the protection of privacy rights in some contexts, we must recognize anonymity as one conception of privacy: see E. Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000), 50 *U.T.L.J.* 305, at pp. 325-26; Westin, at p. 32; Gutterman, at p. 706.

[45] Recognizing that anonymity is one conception of informational privacy seems to me to be particularly important in the context of Internet usage. One form of anonymity, as Westin explained, is what is claimed by an individual who wants to present ideas publicly but does not want to be identified as their author: p. 32. Here, Westin, publishing in 1970, anticipates precisely one of the defining characteristics of some types of Internet communication. The communication may be accessible to millions of people but it is not identified with its author.

[46] Moreover, the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. "Cookies" may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided: see N. Gleicher, "Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web" (2009), 118 *Yale L.J.* 1945, at pp. 1948-49; R. W. Hubbard, P. DeFreitas and S. Magotiaux, "The Internet — Expectations of Privacy in a New Context" (2002), 45 *Crim. L.Q.* 170, at pp. 189-91. The user cannot fully control or even necessarily be aware of who

pas qu'elle renonce à tous ses droits en matière de vie privée, même si, en pratique, il se peut qu'elle ne soit pas en mesure d'exercer un contrôle à l'égard des personnes qui l'observent en public. Par conséquent, pour protéger les droits en matière de vie privée dans certains contextes, il nous faut reconnaître l'anonymat comme une des conceptions de la vie privée : voir E. Paton-Simpson, « Privacy and the Reasonable Paranoid : The Protection of Privacy in Public Places » (2000), 50 *U.T.L.J.* 305, p. 325-326; Westin, p. 32; Gutterman, p. 706.

[45] S'agissant de l'utilisation d'Internet, il me semble particulièrement important de reconnaître que l'anonymat s'inscrit parmi les conceptions de l'aspect informationnel du droit à la vie privée. Comme l'explique le professeur Westin, l'anonymat porte entre autres sur le droit revendiqué par une personne qui veut présenter publiquement ses idées sans être identifiée comme leur auteur : p. 32. Le professeur Westin, dont l'ouvrage a été publié en 1970, avait anticipé précisément une des caractéristiques déterminantes de certains types de communication par Internet. En effet, des millions de personnes peuvent avoir accès à une communication qui n'est toutefois pas associée à son auteur.

[46] De plus, Internet a augmenté de façon exponentielle la qualité et la quantité des renseignements stockés concernant les internautes. L'historique de navigation, par exemple, permet d'obtenir des renseignements détaillés sur les intérêts des utilisateurs. Les moteurs de recherche peuvent recueillir des renseignements sur les termes recherchés par les utilisateurs. Les annonceurs peuvent suivre leurs utilisateurs à travers les réseaux de sites Web et obtenir un aperçu de leurs intérêts et de leurs préoccupations. Les fichiers témoins peuvent être utilisés pour suivre les habitudes de consommation et peuvent fournir des renseignements sur les options sélectionnées dans un site Web, sur les pages Web consultées avant et après avoir visité le site d'accueil et tout autre renseignement personnel fourni : voir N. Gleicher, « Neither a Customer Nor a Subscriber Be : Regulating the Release of User Information on the World Wide Web » (2009), 118 *Yale L.J.* 1945, p. 1948-1949; R. W. Hubbard, P. DeFreitas et S. Magotiaux, « The Internet — Expectations of

may observe a pattern of online activity, but by remaining anonymous — by guarding the link between the information and the identity of the person to whom it relates — the user can in large measure be assured that the activity remains private: see Slane and Austin, at pp. 500-3.

[47] In my view, the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. A sniffer dog provides information about the contents of the bag and therefore engages the privacy interests relating to its contents. DRA readings provide information about what is going on inside a home and therefore may engage the privacy interests relating to those activities. Similarly, subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information.

[48] Doherty J.A. made this point with his usual insight and clarity in *Ward*. "Personal privacy" he wrote "protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society": para. 71. He concluded that some degree of anonymity is a feature of much Internet activity and that, "[d]epending on the totality of the circumstances, . . . anonymity may enjoy constitutional protection under s. 8": para. 75. I agree. Thus, anonymity may, depending on the

Privacy in a New Context » (2002), 45 *Crim. L.Q.* 170, p. 189-191. L'utilisateur n'est pas en mesure d'exercer un contrôle total à l'égard de la personne qui peut observer le profil de ses activités en ligne et il n'est pas toujours informé de l'identité de celle-ci. Or, sous le couvert de l'anonymat — en protégeant le lien entre l'information et l'identité de la personne qu'elle concerne —, l'utilisateur peut en grande partie être assuré que ses activités demeurent confidentielles : voir Slane et Austin, p. 500-503.

[47] À mon avis, il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de téléphone qui figurent parmi les renseignements relatifs à l'abonné. Un chien renifleur fournit de l'information sur le contenu d'un sac et met donc en jeu des droits en matière de vie privée relativement à ce contenu. Les enregistrements de l'AN fournissent de l'information sur les activités qui se déroulent à l'intérieur d'une résidence et peuvent donc mettre en jeu des droits en matière de vie privée concernant ces activités. Dans le même ordre d'idées, en établissant un lien entre des renseignements particuliers et une personne identifiable, les renseignements relatifs à l'abonné peuvent compromettre les droits en matière de vie privée de cette personne non seulement parce qu'ils révèlent son nom et son adresse, mais aussi parce qu'ils l'identifient en tant que source, possesseur ou utilisateur des renseignements visés.

[48] Dans *Ward*, le juge Doherty, clair et lucide comme à son habitude, a fourni des explications semblables. [TRADUCTION] « Le droit à la vie privée », a-t-il écrit, « permet à une personne de fonctionner au quotidien dans la société tout en bénéficiant d'un certain degré d'anonymat indispensable à son épanouissement personnel ainsi qu'à l'épanouissement d'une société ouverte et démocratique » : par. 71. Il a conclu qu'un certain degré d'anonymat est propre à beaucoup d'activités exercées sur Internet et que, « [e]u égard à l'ensemble des circonstances, [. . .] l'anonymat peut bénéficier de

totality of the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure.

[49] The intervener the Director of Public Prosecutions raised the concern that recognizing a right to online anonymity would carve out a crime-friendly Internet landscape by impeding the effective investigation and prosecution of online crime. In light of the grave nature of the criminal wrongs that can be committed online, this concern cannot be taken lightly. However, in my view, recognizing that there *may* be a privacy interest in anonymity depending on the circumstances falls short of recognizing any "right" to anonymity and does not threaten the effectiveness of law enforcement in relation to offences committed on the Internet. In this case, for example, it seems clear that the police had ample information to obtain a production order requiring Shaw to release the subscriber information corresponding to the IP address they had obtained.

[50] Applying this framework to the facts of the present case is straightforward. In the circumstances of this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances as engaging significant privacy interests: *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 3; *Cole*, at para. 47; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at paras. 40-45.

la protection constitutionnelle prévue à l'art. 8 » : par. 75. Je suis d'accord. L'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée visé par la protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives.

[49] Le directeur des poursuites pénales, intervenant, a fait valoir que la reconnaissance du droit à l'anonymat en ligne transformerait Internet en un endroit favorable aux actes criminels en faisant obstacle aux enquêtes et aux poursuites efficaces des cybercrimes. Compte tenu de la gravité des actes criminels qui peuvent être perpétrés en ligne, cette préoccupation ne peut être prise à la légère. J'estime toutefois que la reconnaissance de la *possibilité* qu'il existe un intérêt en matière de vie privée à l'égard de l'anonymat, selon les circonstances, ne suffit pas pour reconnaître le « droit » à l'anonymat et n'a pas pour effet de menacer l'efficacité des autorités d'application de la loi relativement aux infractions commises sur Internet. En l'espèce, par exemple, il semble évident que la police disposait de renseignements détaillés permettant d'obtenir une ordonnance de communication enjoignant à Shaw de fournir les renseignements sur l'abonnée à qui appartenait l'adresse IP qu'elle avait obtenue.

[50] L'application de ce cadre d'analyse aux faits de la présente affaire est simple. Dans les circonstances de l'espèce, la demande de la police dans le but d'établir un lien entre une adresse IP donnée et les renseignements relatifs à l'abonnée visait en fait à établir un lien entre une personne précise (ou un nombre restreint de personnes dans le cas des services Internet partagés) et des activités en ligne précises. Ce genre de demande porte sur l'aspect informationnel du droit à la vie privée relatif à l'anonymat en cherchant à établir un lien entre le suspect et des activités entreprises en ligne, sous le couvert de l'anonymat, activités qui, comme la Cour l'a reconnu dans d'autres circonstances, mettent en jeu d'importants droits en matière de vie privée : *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, par. 3; *Cole*, par. 47; *R. c. Vu*, 2013 CSC 60, [2013] 3 R.C.S. 657, par. 40-45.

[51] I conclude therefore that the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet activity engages a high level of informational privacy. I agree with Caldwell J.A.'s conclusion on this point:

> . . . a reasonable and informed person concerned about the protection of privacy would expect one's activities on one's own computer used in one's own home would be private. . . . In my judgment, it matters not that the personal attributes of the Disclosed Information pertained to Mr. Spencer's sister because Mr. Spencer was personally and directly exposed to the consequences of the police conduct in this case. As such, the police conduct *prima facie* engaged a personal privacy right of Mr. Spencer and, in this respect, his interest in the privacy of the Disclosed Information was direct and personal. [para. 27]

(c) *Reasonable Expectation of Privacy*

[52] The next question is whether Mr. Spencer's expectation of privacy was reasonable. The trial judge found that there could be no reasonable expectation of privacy in the face of the relevant contractual and statutory provisions (para. 19), a conclusion with which Caldwell J.A. agreed on appeal: para. 42. Cameron J.A., however, was doubtful that the contractual and statutory terms had this effect in the context of this case: para. 98.

[53] In this Court, Mr. Spencer maintains that the contractual and statutory terms did not undermine a reasonable expectation of privacy with respect to the subscriber information. He submits that the contractual provisions do nothing more than suggest that the information will not be provided to police unless required by law and that *PIPEDA*, whose purpose is to protect privacy rights, supports rather than negates the reasonableness of an expectation of privacy in this case. The Crown

[51] Par conséquent, je conclus que la demande de la police auprès de Shaw — visant à obtenir des renseignements relatifs à l'abonnée qui correspondaient à des activités entreprises sur Internet de façon anonyme et observées en particulier — fait intervenir, dans une grande mesure, l'aspect informationnel du droit à la vie privée. Je souscris à la conclusion du juge Caldwell sur ce point :

> [TRADUCTION] . . . une personne raisonnable et bien informée, qui se soucie de la protection de la vie privée, s'attendrait à ce que les activités qu'une personne effectue sur son propre ordinateur et dans son domicile soient confidentielles. [. . .] À mon avis, il n'importe nullement que les renseignements communiqués concernaient la sœur de M. Spencer parce que, en l'espèce, M. Spencer a, personnellement et directement, subi les conséquences des actes de la police. À première vue, ces actes font intervenir le droit de M. Spencer à la vie privée et, de ce fait, son intérêt en matière de vie privée relativement à la confidentialité des renseignements communiqués était direct et personnel. [par. 27]

c) *L'attente raisonnable en matière de respect de la vie privée*

[52] Il s'agit maintenant de savoir si l'attente de M. Spencer en matière de respect de sa vie privée était raisonnable. Selon le juge du procès, il ne pouvait pas y avoir d'attente raisonnable en matière de respect de la vie privée compte tenu des dispositions contractuelles et législatives applicables (par. 19), conclusion à laquelle le juge Caldwell a souscrit en appel : par. 42. Le juge Cameron a affirmé douter pour sa part que les dispositions du contrat et celles de la loi aient cet effet dans le contexte de la présente affaire : par. 98.

[53] Devant la Cour, M. Spencer a fait valoir que les dispositions du contrat et de la loi n'ont pas pour effet de compromettre une attente raisonnable en matière de vie privée relativement aux renseignements relatifs à l'abonné. Selon lui, les dispositions du contrat ne font rien d'autre qu'indiquer qu'il n'y aura pas de communication des renseignements à la police, à moins que cela ne soit requis par la loi, et que la *LPRPDE* — qui vise à protéger les droits en matière de vie privée — tend

disagrees and supports the position taken on this point by Caldwell J.A. in the Court of Appeal.

[54] There is no doubt that the contractual and statutory framework may be relevant to, but not necessarily determinative of, whether there is a reasonable expectation of privacy. So, for example in *Gomboc*, Deschamps J. writing for four members of the Court, found that the terms governing the relationship between the electricity provider and its customer were "highly significant" to Mr. Gomboc's reasonable expectation of privacy, but treated it as "one factor amongst many which must be weighed in assessing the totality of the circumstances": paras. 31-32. She also emphasized that when dealing with contracts of adhesion in the context of a consumer relationship, it was necessary to "procee[d] with caution" when determining the impact that such provision would have on the reasonableness of an expectation of privacy: para. 33. The need for caution in this context was pointedly underlined in the dissenting reasons of the Chief Justice and Fish J. in that case: paras. 138-42.

[55] The contractual and statutory frameworks overlap in the present case because the Shaw Joint Terms of Service make reference to *PIPEDA*, and the scope of permitted disclosure under *PIPEDA* turns partly on whether the customer has consented to the disclosure of personal information. I must first set out the details of these schemes before turning to their impact on the reasonable expectations analysis. In doing so, it becomes apparent that the relevant provisions provide little assistance in evaluating the reasonableness of Mr. Spencer's expectation of privacy.

[56] Shaw provides Internet services to its customers under a standard form "Joint Terms of

à confirmer plutôt qu'à nier le caractère raisonnable d'une attente en matière de vie privée en l'espèce. Le ministère public ne souscrit pas à cet argument et appuie la position adoptée sur ce point par le juge Caldwell de la Cour d'appel.

[54] Il ne fait aucun doute que les cadres législatif et contractuel peuvent être pertinents, mais pas nécessairement déterminants, quant à la question de savoir s'il existe une attente raisonnable en matière de vie privée. Dans l'arrêt *Gomboc*, par exemple, s'exprimant au nom de quatre juges de la Cour, la juge Deschamps a conclu que les dispositions régissant les rapports entre le fournisseur d'électricité et son client revêtent une « grande importance » quant à l'attente raisonnable de M. Gomboc en matière de vie privée, mais a considéré qu'il s'agissait d'« un des nombreux facteurs dont il faut tenir compte pour apprécier l'ensemble des circonstances » : par. 31-32. La juge Deschamps a également souligné que, dans le cadre de contrats d'adhésion qui régissent les relations avec les clients, « la prudence est évidemment de mise » lorsqu'il s'agit de juger des conséquences que peuvent avoir les dispositions de ces contrats sur le caractère raisonnable d'une attente en matière de respect de la vie privée : par. 33. Dans leurs motifs dissidents, la Juge en chef et le juge Fish ont mis l'accent sur le besoin de faire preuve de prudence dans ce contexte : par. 138-142.

[55] En l'espèce, les cadres contractuel et législatif se chevauchent parce que les conditions de service de Shaw renvoient à la *LPRPDE* et que la portée de la communication autorisée de renseignements personnels sous le régime de la *LPRPDE* repose en partie sur la question de savoir si le client a donné son consentement à cet égard. Avant d'examiner les conséquences de ces régimes sur l'analyse relative aux attentes raisonnables en matière de vie privée, je dois en préciser les modalités. Lorsque je le fais, il devient clair que les dispositions applicables ne sont guère utiles pour évaluer le caractère raisonnable de l'attente de M. Spencer au respect de sa vie privée.

[56] Shaw fournit des services Internet à ses clients conformément à une entente type relative

Service" agreement. Additional terms and conditions are provided in Shaw's "Acceptable Use Policy" and its "Privacy Policy". The terms of these agreements are posted online on Shaw's website and change from time to time. The investigators sought the subscriber information for the IP address used on August 31, 2007 in their request to Shaw.

aux « Conditions de service » (« *Joint Terms of Service* »). Sa [TRADUCTION] « Politique relative à l'utilisation acceptable » (« *Acceptable Use Policy* ») et sa « Politique sur la protection de la vie privée » (« *Privacy Policy* ») prévoient des modalités et conditions supplémentaires. Les dispositions de ces ententes sont affichées en ligne sur le site Web de Shaw et font périodiquement l'objet de modifications. Les enquêteurs ont demandé à Shaw des renseignements sur l'abonnée à qui appartenait l'adresse IP utilisée le 31 août 2007.

[57] Mr. Spencer was not personally a party to these agreements, as he accessed the Internet through his sister's subscription. It is common practice for multiple users to share a common Internet connection. A reasonable user would be aware that the use of the service would be governed by certain terms and conditions, and those terms and conditions were readily accessible through Shaw's website. This case does not require us to decide whether Mr. Spencer was bound by the terms of the contract with Shaw. Quite apart from contractual liability, the terms on which he gained access to the Internet are a relevant circumstance in assessing the reasonableness of his expectation of privacy. There are three relevant sets of provisions which, taken as a whole, provide a confusing and unclear picture of what Shaw would do when faced with a police request for subscriber information. The Joint Terms of Service at first blush appear to permit broad disclosure because they provide, among other things, that "Shaw may disclose any information as is necessary to . . . satisfy any legal, regulatory or other governmental request". This general provision, however, must be read in light of the more specific provision relating to disclosure of IP addresses and other identifying information in the context of criminal investigations contained in the Acceptable Use Policy, which in turn is subject to the Privacy Policy.

[57] Monsieur Spencer n'était pas lui-même partie à ces ententes, puisqu'il avait accès à Internet au moyen de l'abonnement de sa sœur. Il est d'ailleurs très courant que plusieurs utilisateurs partagent une connexion Internet. L'usager raisonnable sait que l'utilisation du service Internet est régie par certaines modalités, qui étaient d'ailleurs facilement accessibles sur le site Web de Shaw. Nous n'avons toutefois pas à décider en l'espèce si M. Spencer était lié par les modalités du contrat avec Shaw. Cependant, indépendamment de la responsabilité contractuelle, les conditions auxquelles il a pu accéder à Internet sont pertinentes pour évaluer le caractère raisonnable de son attente quant au respect de sa vie privée. Il existe trois séries de dispositions applicables qui, dans leur ensemble, prêtent à confusion quant à la manière de Shaw de répondre à une demande de renseignements relatifs à un abonné adressée par la police. À première vue, les Conditions de service semblent conférer à Shaw un vaste pouvoir discrétionnaire parce qu'elles prévoient, entre autres, qu'[TRADUCTION] « [elle] peut communiquer les renseignements nécessaires pour [. . .] satisfaire à toute demande fondée sur une loi ou un règlement ou toute autre demande du gouvernement ». Il convient toutefois d'interpréter cette disposition générale en fonction de la disposition plus spécifique concernant la communication d'adresses IP et d'autres renseignements personnels dans le contexte d'enquêtes criminelles qui figure dans la Politique relative à l'utilisation acceptable qui, elle-même, est assujettie à la Politique sur la protection de la vie privée.

[58] The Acceptable Use Policy (last updated on June 18, 2007) provides that Shaw is authorized

[58] Suivant la Politique relative à l'utilisation acceptable (dont la mise à jour la plus récente date

to cooperate with law enforcement authorities in the investigation of criminal violations, including supplying information identifying a subscriber *in accordance with its Privacy Policy*. The provision reads as follows:

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. [Emphasis added.]

[59] The Privacy Policy in the record (last updated on November 12, 2008) states that Shaw is committed to protecting personal information, which is defined as information about an identifiable individual. One of the ten principles set out in the Privacy Policy deals with limiting the disclosure of personal information (principle 5). The policy limits the circumstances under which personal information will be disclosed without the customer's knowledge or consent to "exceptional circumstances, as permitted by law". Shaw may disclose information to its partners in order to provide its services and, in such cases, the information is governed by "strict confidentiality standards and policies" to keep the information secure and to ensure it is treated in accordance with *PIPEDA*. The Privacy Policy also provides that "Shaw may disclose Customer's Personal Information to: . . . a third party or parties, where the Customer has given Shaw Consent to such disclosure or if disclosure is required by law, in accordance with *The Personal Information Protection and Electronic Documents Act*" (emphasis added).

du 18 juin 2007), Shaw est autorisée à collaborer avec les autorités d'application de la loi dans le cadre d'enquêtes sur des infractions criminelles, notamment en fournissant des renseignements personnels sur un abonné, *conformément à sa Politique sur la protection de la vie privée*. Cette disposition est ainsi libellée :

[TRADUCTION] Par la présente, vous autorisez Shaw à collaborer avec (i) les autorités d'application de la loi dans le cadre d'enquêtes sur des infractions criminelles présumées, et avec (ii) les administrateurs du système d'autres fournisseurs de services Internet ou d'autres réseaux ou installations informatiques afin de faire appliquer la présente entente. Cette collaboration peut comprendre la communication du nom d'utilisateur, de l'adresse IP ou d'autres renseignements personnels concernant un abonné, conformément aux lignes directrices énoncées dans sa Politique sur la protection de la vie privée. [Je souligne.]

[59] Suivant la Politique sur la protection de la vie privée qui figure au dossier (dont la mise à jour la plus récente date du 12 novembre 2008), Shaw s'engage à protéger les renseignements personnels, définis comme des renseignements concernant un individu identifiable. Un des dix principes énoncés dans la Politique sur la protection de la vie privée a pour effet de restreindre la communication de renseignements personnels (principe n^{o} 5). Cette politique limite les circonstances dans lesquelles les renseignements personnels seront communiqués à l'insu du client ou sans son consentement à des [TRADUCTION] « circonstances exceptionnelles, conformément à la loi ». Shaw peut communiquer des renseignements à ses partenaires afin de fournir ses services, et, dans de tels cas, ces renseignements sont régis par des « normes et politiques strictes en matière de confidentialité » pour assurer leur sécurité et pour veiller à ce qu'ils soient traités conformément à la *LPRPDE*. La Politique sur la protection de la vie privée prévoit également que « Shaw peut communiquer des renseignements personnels concernant un client : [. . .] à une partie ou à plusieurs tierces parties lorsque le client visé a donné son consentement à cet égard ou lorsque la communication des renseignements est exigée par la loi, conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* » (je souligne).

[60] Whether or not disclosure of personal information by Shaw is "permitted" or "required by law" in turn depends on an analysis of the applicable statutory framework. The contractual provisions, read as a whole, are confusing and equivocal in terms of their impact on a user's reasonable expectation of privacy in relation to police initiated requests for subscriber information. The statutory framework provided by *PIPEDA* is not much more illuminating.

[61] Shaw's collection, use, and disclosure of the personal information of its subscribers is subject to *PIPEDA*, which protects personal information held by organizations engaged in commercial activities from being disclosed without the knowledge or consent of the person to whom the information relates: Sch. 1, clause 4.3. Section 7 contains several exceptions to this general rule and permits organizations to disclose personal information without consent. The exception relied on in this case is s. 7(3)(*c.*1)(ii). It permits disclosure to a government institution that has requested the disclosure for the purpose of law enforcement and has stated its "lawful authority" for the request. The provisions of *PIPEDA* are not of much help in determining whether there is a reasonable expectation of privacy in this case. They lead us in a circle.

[62] Section 7(3)(*c.*1)(ii) allows for disclosure without consent to a government institution where that institution has identified its *lawful authority* to obtain the information. But the issue is whether there was such lawful authority which in turn depends in part on whether there was a reasonable expectation of privacy with respect to the subscriber information. *PIPEDA* thus cannot be used as a factor to weigh against the existence of a reasonable expectation of privacy since the

[60] Ainsi, la réponse à la question de savoir si la communication des renseignements personnels par Shaw est « autorisée » ou « exigée par la loi » repose sur l'analyse du cadre législatif applicable. Les dispositions du contrat, lues conjointement, sont équivoques et prêtent à confusion quant à leurs conséquences sur l'attente raisonnable de l'utilisateur en matière de vie privée relativement aux demandes de la police visant à obtenir des renseignements relatifs à l'abonné. Le cadre législatif prévu par la *LPRPDE* ne permet pas d'en apprendre davantage.

[61] La collecte, l'utilisation et la communication par Shaw de renseignements personnels concernant ses abonnés sont assujetties à la *LPRPDE*, laquelle protège les renseignements personnels que possèdent les organisations qui exercent des activités commerciales contre leur communication à l'insu de l'intéressé et sans son consentement : ann. 1, art. 4.3. L'article 7 prévoit plusieurs exceptions à cette règle générale, permettant ainsi aux organisations de communiquer des renseignements personnels sans le consentement de l'intéressé. L'exception invoquée en l'espèce figure au sous-al. 7(3)*c.*1)(ii), qui autorise la communication de renseignements à une institution gouvernementale qui a demandé à obtenir les renseignements visés aux fins du contrôle d'application du droit en mentionnant la « source de l'autorité légitime » étayant la demande. En l'espèce, les dispositions de la *LPRPDE* ne sont pas très utiles pour déterminer s'il existe une attente raisonnable en matière de vie privée puisqu'après les avoir examinées, on se retrouve au point de départ.

[62] Le sous-alinéa 7(3)*c.*1)(ii) autorise la communication de renseignements, sans le consentement de l'intéressé, faite à une institution gouvernementale lorsque cette dernière mentionne la *source de l'autorité légitime* étayant son droit à obtenir les renseignements demandés. Il s'agit toutefois de savoir s'il existe une telle source d'autorité légitime, question dont la réponse dépend, en partie, de l'existence d'une attente raisonnable en matière de vie privée à l'égard des renseignements concernant

proper interpretation of the relevant provision itself depends on whether such a reasonable expectation of privacy exists. Given that the purpose of *PIPEDA* is to establish rules governing, among other things, disclosure "of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information" (s. 3), it would be reasonable for an Internet user to expect that a simple request by police would not trigger an obligation to disclose personal information or defeat *PIPEDA*'s general prohibition on the disclosure of personal information without consent.

[63] I am aware that I have reached a different result from that reached in similar circumstances by the Ontario Court of Appeal in *Ward*, where the court held that the provisions of *PIPEDA* were a factor which weighed against finding a reasonable expectation of privacy in subscriber information. This conclusion was based on two main considerations. The first was that an ISP has a legitimate interest in assisting in law enforcement relating to crimes committed using its services: para. 99. The second was the grave nature of child pornography offences, which made it reasonable to expect that an ISP would cooperate with a police investigation: paras. 102-3. While these considerations are certainly relevant from a policy perspective, they cannot override the clear statutory language of s. 7(3)(*c.*1)(ii) of *PIPEDA*, which permits disclosure only if a request is made by a government institution with "lawful authority" to request the disclosure. It is reasonable to expect that an organization bound by *PIPEDA* will respect its statutory obligations with respect to personal information. The Court of Appeal in *Ward* held that s. 7(3)(*c.*1)(ii) must be read in light of s. 5(3), which states that "[a]n organization may collect, use or disclose personal information only for purposes

l'abonné. La *LPRPDE* ne peut donc être considérée comme un des facteurs défavorables à l'existence d'une attente raisonnable en matière de vie privée puisque l'interprétation juste de la disposition applicable dépend elle-même de l'existence d'une telle attente raisonnable en matière de vie privée. Puisque la *LPRPDE* a pour objet de fixer des règles régissant, entre autres, 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 » (art. 3), il serait raisonnable que l'internaute s'attende à ce qu'une simple demande faite par la police n'entraîne pas l'obligation de communiquer les renseignements personnels en question ou qu'elle n'écarte pas l'interdiction générale prévue par la *LPRPDE* quant à la communication de renseignements personnels sans le consentement de l'intéressé.

[63] Certes, je suis arrivé à une conclusion différente que celle formulée, dans des circonstances semblables, dans l'arrêt *Ward*, où la Cour d'appel de l'Ontario a statué que les dispositions de la *LPRPDE* constituaient un facteur qui pesait contre la reconnaissance de l'existence d'une attente raisonnable en matière de vie privée à l'égard des renseignements concernant l'abonné. Cette conclusion reposait sur deux considérations principales. Premièrement, le fait que le FSI a un intérêt légitime à collaborer avec les autorités d'application de la loi relativement à des crimes commis lors de l'utilisation de ses services : par. 99. Deuxièmement, la gravité des infractions de pornographie juvénile, compte tenu de laquelle il était raisonnable de s'attendre à ce que le FSI collabore avec la police dans le cadre d'une enquête : par. 102-103. Bien qu'elles soient certainement pertinentes sur le plan des principes, ces considérations ne sauraient avoir priorité sur le libellé clair du sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, qui n'autorise la communication de renseignements que lorsqu'une institution gouvernementale mentionne la « source de l'autorité légitime » étayant sa demande. En effet, il est raisonnable de s'attendre à ce qu'une organisation assujettie à la *LPRPDE* respecte les

that a reasonable person would consider are appropriate in the circumstances". This rule of "reasonable disclosure" was used as a basis to invoke considerations such as allowing ISPs to cooperate with the police and preventing serious crimes in the interpretation of *PIPEDA*. Section 5(3) is a guiding principle that underpins the interpretation of the various provisions of *PIPEDA*. It does not allow for a departure from the clear requirement that a requesting government institution possess "lawful authority" and so does not resolve the essential circularity of using s. 7(3)(*c.*1)(ii) as a factor in determining whether a reasonable expectation of privacy exists.

obligations que celle-ci lui impose à l'égard des renseignements personnels. La Cour d'appel a statué dans l'arrêt *Ward* qu'il convient d'interpréter le sous-al. 7(3)*c.*1)(ii) en tenant compte du par. 5(3), suivant lequel « [l']organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ». Cette règle de la « communication raisonnable » a permis de prendre en considération, pour interpréter la *LPRPDE*, des facteurs comme l'autorisation des FSI à collaborer avec la police et la lutte contre les crimes graves. Le paragraphe 5(3) énonce un principe directeur sur lequel repose l'interprétation des diverses dispositions de la *LPRPDE*. Il ne permet pas d'écarter l'exigence claire concernant la « source de l'autorité légitime » qui étaye la demande d'une institution gouvernementale et ne règle donc pas l'impasse que crée le sous-al. 7(3)*c.*1)(ii) pour juger de l'existence ou non d'une attente raisonnable en matière de vie privée.

[64] I also note with respect to an ISP's legitimate interest in preventing crimes committed through its services that entirely different considerations may apply where an ISP itself detects illegal activity and of its own motion wishes to report this activity to the police. Such a situation falls under a separate, broader exemption in *PIPEDA*, namely s. 7(3)(*d*). The investigation in this case was begun as a police investigation and the disclosure of the subscriber information arose out of the request letter sent by the police to Shaw.

[64] Je fais en outre remarquer, au sujet de l'intérêt légitime du FSI dans la lutte contre les crimes commis en utilisant ses services, que des considérations tout à fait différentes peuvent s'appliquer si le FSI détecte lui-même une activité illégale et, de sa propre initiative, souhaite la signaler à la police. Une telle situation tombe sous le coup d'une exemption distincte, plus large, prévue par la *LPRPDE*, à savoir celle énoncée à l'al. 7(3)*d*). En l'espèce, l'enquête a été commencée par la police et la communication des renseignements relatifs à l'abonnée a été faite par suite de la lettre de demande envoyée à Shaw par la police.

[65] The overall impression created by these terms is that disclosure at the request of the police would be made only where required or permitted by law. Such disclosure is only permitted by *PIPEDA* in accordance with the exception in s. 7, which in this case would require the requesting police to have "lawful authority" to request the disclosure. For reasons that I will set out in the next section, this request had no lawful authority in the sense that while the police could ask, they had no authority to compel compliance with that request. I conclude

[65] De ces modalités se dégage l'impression générale que la communication faite à la demande de la police n'aurait lieu que lorsqu'elle est exigée ou autorisée par la loi. Or, la *LPRPDE* n'autorise une telle communication que suivant l'exception prévue à l'art. 7. Il faudrait donc que la police qui formule la demande de communication détienne « l'autorité légitime » à cet égard. Pour les motifs que j'énoncerai dans la prochaine partie, la demande en cause n'était pas étayée par la source de l'autorité légitime de la police, en ce sens que

that, if anything, the contractual provisions in this case support the existence of a reasonable expectation of privacy, since the Privacy Policy narrowly circumscribes Shaw's right to disclose the personal information of subscribers.

[66] In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.

[67] The intervener the Attorney General of Alberta raised a concern that if the police were not permitted to request disclosure of subscriber information, then other routine inquiries that might reveal sensitive information about a suspect would also be prohibited, and this would unduly impede the investigation of crimes. For example, when the police interview the victim of a crime, core biographical details of a suspect's lifestyle might be revealed. I do not agree that this result follows from the principles set out in these reasons. Where a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information: *Plant*, at p. 293; *Gomboc*, at paras. 27-30, *per* Deschamps J. In *Duarte*, the Court distinguished between a person repeating a conversation with a suspect to the police and the police procuring an audio recording of the same conversation. The Court held that the danger is "not the risk that someone will repeat our words but the

cette dernière pouvait formuler une demande, mais ne détenait pas l'autorité pour obliger le fournisseur à s'y conformer. Je conclus que les dispositions du contrat en l'espèce justifient l'existence d'une attente raisonnable en matière de vie privée, si un quelconque effet doit être donné à ces termes en cette matière, puisque la Politique sur la protection de la vie privée a pour effet de limiter strictement le droit de Shaw de communiquer des renseignements personnels concernant ses abonnés.

[66] À mon avis, compte tenu de l'ensemble des circonstances de la présente affaire, il existe une attente raisonnable en matière de vie privée à l'égard des renseignements relatifs à l'abonnée. La communication de ces renseignements permettra souvent d'identifier l'utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes. La demande faite par un policier visant la communication volontaire par le FSI de renseignements de cette nature constitue donc une fouille.

[67] Le procureur général de l'Alberta, intervenant en l'espèce, a dit craindre que, si la police n'était pas autorisée à demander la communication de renseignements relatifs à un abonné donné, d'autres demandes courantes pouvant révéler des renseignements confidentiels sur un suspect risquent d'être également interdites, ce qui aurait pour effet d'entraver indûment l'enquête sur des crimes. Par exemple, lorsque les policiers interrogent la victime d'un crime, des renseignements biographiques d'ordre personnel concernant le mode de vie du suspect pourraient être révélés. Je ne suis pas d'accord pour dire que cette conclusion découle des principes énoncés dans les présents motifs. Pour déterminer si la demande faite par un policier à un tiers de communiquer des renseignements concernant un suspect constitue une fouille ou une perquisition, il faut se demander si, compte tenu de l'ensemble des circonstances, le suspect a une attente raisonnable en matière de vie privée à l'égard de ces renseignements : *Plant*, p. 293; *Gomboc*, par. 27-30, la juge Deschamps. Dans l'arrêt *Duarte*, la Cour a établi une distinction entre une personne

much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words": at pp. 43-44. Similarly in this case, the police request that the ISP disclose the subscriber information was in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police and thus engaged a more significant privacy interest than a simple question posed by the police in the course of an investigation.

B. *Was the Search Lawful?*

[68] A warrantless search, such as the one that occurred in this case, is presumptively unreasonable: *R. v. Collins*, [1987] 1 S.C.R. 265. The Crown bears the burden of rebutting this presumption. A search will be reasonable if (a) it was authorized by law, (b) the law itself was reasonable, and (c) the search was carried out in a reasonable manner: p. 278. Mr. Spencer has not challenged the constitutionality of the laws that purportedly authorized the search. He did raise concerns about the reasonableness of the manner, but in my view, these are groundless. Accordingly, we need only consider whether the search was authorized by law.

[69] The Crown supports the conclusions of Caldwell and Cameron JJ.A. in the Court of Appeal that any search was lawful, relying on the combined effect of s. 487.014 of the *Criminal Code* and s. 7(3)(*c*.1)(ii) of *PIPEDA*. I respectfully do not agree.

[70] Section 487.014(1) of the *Criminal Code* provides that a peace officer does not need a production order "to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from

qui rapporte à la police une conversation avec un suspect et l'enregistrement par la police de la même conversation. Selon la Cour, il s'agit « non plus [du] risque que quelqu'un répète nos propos, mais [du] danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos » : p. 43-44. De même, dans l'affaire qui nous occupe, la demande par la police que le FSI communique les renseignements relatifs à l'abonnée constituait en fait une demande d'établir un lien entre M. Spencer et des activités précises menées en ligne qui avaient été surveillées par police, et mettait donc en jeu un droit en matière de vie privée beaucoup plus important qu'une simple question formulée lors d'une enquête policière.

B. *La fouille était-elle légitime?*

[68] Une fouille sans mandat, comme celle qui a été effectuée en l'espèce, est présumée abusive : *R. c. Collins*, [1987] 1 R.C.S. 265. Il incombe au ministère public de réfuter cette présomption. Une fouille ne sera pas abusive si a) elle est autorisée par la loi, b) la loi elle-même n'a rien d'abusif, et c) la fouille n'a pas été effectuée d'une manière abusive : p. 278. M. Spencer ne conteste pas la constitutionnalité des lois qui auraient autorisé la fouille. Il a toutefois soulevé des objections quant à la manière, qu'il estime abusive, dont a été effectuée la fouille. À mon avis, ces objections sont mal fondées. Il ne reste donc qu'à examiner si la fouille était autorisée par la loi.

[69] Le ministère public appuie les conclusions tirées par les juges Caldwell et Cameron de la Cour d'appel selon lesquelles la fouille était légitime, compte tenu de l'effet combiné de l'art. 487.014 du *Code criminel* et du sous-al. 7(3)*c*.1)(ii) de la *LPRPDE*. En toute déférence, je ne souscris pas à cette opinion.

[70] Suivant le par. 487.014(1) du *Code criminel*, une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix « demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune

disclosing". *PIPEDA* prohibits disclosure of the information unless the requirements of the law enforcement provision are met, including that the government institution discloses a lawful authority *to obtain*, not simply to ask for the information: s. 7(3)(*c.*1)(ii). On the Crown's reading of these provisions, *PIPEDA*'s protections become virtually meaningless in the face of a police request for personal information: the "lawful authority" is a simple request without power to compel and, because there was a simple request, the institution is no longer prohibited by law from disclosing the information.

règle de droit n'interdit à celle-ci de communiquer ». La *LPRPDE* interdit la communication de renseignements à moins que les autorités d'application de la loi ne respectent les exigences les concernant, notamment l'exigence selon laquelle une institution gouvernementale doit mentionner la source de l'autorité légitime étayant son droit *d'obtenir* les renseignements, et non seulement de les demander : sous-al. 7(3)*c.*1)(ii). Selon l'interprétation que donne le ministère public de ces dispositions, une demande de renseignements personnels faite par la police rendrait pratiquement sans effet les protections prévues par la *LPRPDE* : l'exigence relative à la « source de l'autorité légitime » ne constitue qu'une simple demande sans aucun pouvoir de contrainte, mais, par suite d'une simple demande, la communication de renseignements par l'institution en question n'est plus prohibée par la loi.

[71] "Lawful authority" in s. 7(3)(*c.*1)(ii) of *PIPEDA* must be contrasted with s. 7(3)(*c*), which provides that personal information may be disclosed without consent where "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". The reference to "lawful authority" in s. 7(3)(*c.*1)(ii) must mean something other than a "subpoena or [search] warrant". "Lawful authority" may include several things. It may refer to the common law authority of the police to ask questions relating to matters that are not subject to a reasonable expectation of privacy. It may refer to the authority of police to conduct warrantless searches under exigent circumstances or where authorized by a reasonable law: *Collins*. As the intervener the Privacy Commissioner of Canada submitted, interpreting "lawful authority" as requiring more than a bare request by law enforcement gives this term a meaningful role to play in the context of s. 7(3) and should be preferred over alternative meanings that do not do so. In short, I agree with the Ontario Court of Appeal in *Ward* on this point that neither s. 487.014(1) of the *Criminal Code*, nor *PIPEDA*

[71] Il faut distinguer la « source de l'autorité légitime » à laquelle réfère le sous-al. 7(3)*c.*1)(ii) de la *LPRPDE* et l'al. 7(3)*c*), selon lequel la communication des renseignements personnels peut être faite sans le consentement de l'intéressé lorsqu'« 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 ». Le renvoi à la « source de l'autorité légitime » au sous-al. 7(3)*c.*1)(ii) doit viser autre chose qu'une « assignation » ou un « mandat » de perquisition. La « source de l'autorité légitime » peut avoir plusieurs sens. Cette notion peut désigner le pouvoir conféré par la common law aux policiers de poser des questions portant sur des éléments qui ne font pas l'objet d'une attente raisonnable en matière de vie privée. Elle peut renvoyer au pouvoir de la police d'effectuer une fouille ou une perquisition sans mandat dans des circonstances contraignantes ou dans des cas où une loi qui n'a rien d'abusif le permet : *Collins*. Comme le fait valoir la commissaire à la protection de la vie privée du Canada, intervenante en l'espèce, si on tient pour acquis que la « source de l'autorité légitime »

creates any police search and seizure powers: para. 46.

[72] I recognize that this conclusion differs from that of the Saskatchewan Court of Appeal in *Trapp*, at para. 66, and the British Columbia Supreme Court in *R. v. McNeice*, 2010 BCSC 1544 (CanLII), at para. 43. The Court of Appeal in *Trapp* read s. 487.014(1) together with s. 29(2)(g) of *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, an analogous provision to s. 7(3)(*c.*1)(ii) of *PIPEDA*, although one from which the "lawful authority" requirement is absent. The court held that s. 487.014(1) gave the police a power to make any inquiries that were not otherwise prohibited by law. The court in *McNeice* took the same approach, although that case concerned s. 7(3)(*c.*1)(ii) of *PIPEDA*, the same provision at issue in this case.

[73] With respect, I cannot accept that this conclusion applies to s. 7(3)(*c.*1)(ii) of *PIPEDA*. Section 487.014(1) is a declaratory provision that confirms the existing common law powers of police officers to make enquiries, as indicated by the fact that the section begins with the phrase "[f]or greater certainty": see *Ward*, at para. 49. *PIPEDA* is a statute whose purpose, as set out in s. 3, is to increase the protection of personal information. Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and

nécessite davantage qu'une simple demande faite par les autorités d'application de la loi, cette notion arrive à jouer un rôle significatif dans le contexte du par. 7(3), au détriment d'autres interprétations qui n'ont pas cet effet. Bref, je suis d'accord avec la Cour d'appel de l'Ontario dans l'arrêt *Ward* sur ce point, pour dire que ni le par. 487.014(1) du *Code criminel* ni la *LPRPDE* n'ont pour effet de conférer à la police des pouvoirs en matière de fouilles, de perquisitions ou de saisies : par. 46.

[72] Je reconnais que cette conclusion diffère de celle tirée par la Cour d'appel de la Saskatchewan dans *Trapp*, par. 66, et par la Cour suprême de la Colombie-Britannique dans *R. c. McNeice*, 2010 BCSC 1544 (CanLII), par. 43. Dans l'arrêt *Trapp*, la Cour d'appel a interprété le par. 487.014(1) de concert avec l'al. 29(2)(g) de la *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, ch. F-22.01, disposition analogue à celle énoncée au sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, même si l'exigence relative à la « source de l'autorité légitime » y est absente. La cour a affirmé que le par. 487.014(1) conférait aux policiers le pouvoir de faire toute demande qui n'était pas prohibée par la loi. La Cour suprême de la Colombie-Britannique a adopté la même approche dans l'affaire *McNeice*, même si celle-ci portait sur le sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*, disposition qui est en cause dans le présent pourvoi.

[73] En toute déférence, je ne peux accepter que cette conclusion s'applique au sous-al. 7(3)*c.*1)(ii) de la *LPRPDE*. Le paragraphe 487.014(1) est une disposition déclaratoire qui confirme les pouvoirs de common law permettant aux policiers de formuler des questions, comme l'indique les premiers mots de son libellé en français « [i]l demeure entendu qu[e] » ou de son libellé en anglais « [f]or greater certainty » : voir *Ward*, par. 49. La *LPRPDE* est une loi qui a pour objet, comme il est indiqué à l'art. 3, d'accroître la protection des renseignements personnels. Puisque, en l'espèce, les policiers n'avaient pas le pouvoir d'effectuer une fouille ou une perquisition pour obtenir des renseignements relatifs à l'abonnée en l'absence de circonstances

a provision enacted to promote the protection of personal information.

[74] The subscriber information obtained by police was used in support of the Information to Obtain which led to the issuance of a warrant to search Ms. Spencer's residence. Without that information, the warrant could not have been obtained. It follows that if that information is excluded from consideration as it must be because it was unconstitutionally obtained, there were not adequate grounds to sustain the issuance of the warrant, and the search of the residence was therefore unlawful. I conclude, therefore, that the conduct of the search of Ms. Spencer's residence violated the *Charter*: *Plant*, at p. 296; *Hunter v. Southam*, at p. 161. Nothing in these reasons addresses or diminishes any existing powers of the police to obtain subscriber information in exigent circumstances such as, for example, where the information is required to prevent imminent bodily harm. There were no such circumstances here.

C. *Should the Evidence Have Been Excluded*

[75] Neither the trial judge nor the Court of Appeal found a breach of s. 8 in this case and, therefore, did not have to consider the question of whether the evidence obtained in a manner that violated Mr. Spencer's *Charter* rights should be excluded under s. 24(2) of the *Charter*. The question is whether the admission of the evidence would bring the administration of justice into disrepute. I accept, as both Mr. Spencer and the Crown agree, that we can determine this issue on the record before us. However, I disagree with Mr. Spencer's submission that the evidence should be excluded. In my view, it should not.

contraignantes ou d'une loi qui n'a rien d'abusif, je ne vois pas comment ils pourraient obtenir un nouveau pouvoir en matière de fouille ou de perquisition par l'effet combiné d'une disposition déclaratoire et d'une disposition adoptée afin de favoriser la protection des renseignements personnels.

[74] La police a utilisé les renseignements relatifs à l'abonnée pour étayer la dénonciation qui a conduit à la délivrance d'un mandat l'autorisant à perquisitionner dans la résidence de M^me^ Spencer. En l'absence de ces renseignements, la police n'aurait pas pu obtenir le mandat. Par conséquent, si ces renseignements sont écartés (ce qui doit être le cas, parce qu'ils ont été obtenus d'une façon inconstitutionnelle), il n'y avait aucun motif valable justifiant la délivrance d'un mandat et la fouille ou la perquisition à la résidence était abusive. Je conclus donc que l'exécution de la fouille ou de la perquisition à la résidence de M^me^ Spencer violait la *Charte* : *Plant*, p. 296; *Hunter c. Southam*, p. 161. Rien dans les présents motifs ne porte sur les pouvoirs dont disposent les policiers pour obtenir des renseignements relatifs à un abonné dans des circonstances contraignantes, par exemple, lorsqu'il est nécessaire d'obtenir de tels renseignements pour prévenir un préjudice physique imminent, ce qui n'était pas le cas en l'espèce. Rien non plus, dans les présents motifs, ne restreint ces pouvoirs.

C. *La preuve aurait-elle dû être écartée?*

[75] Ni le juge du procès ni la Cour d'appel n'ont conclu qu'il y avait violation de l'art. 8 en l'espèce. Ils n'avaient donc pas à se demander si les éléments de preuve obtenus d'une façon qui portait atteinte aux droits de M. Spencer garantis par la *Charte* devraient être écartés en application du par. 24(2) de la même *Charte*. Il s'agit de savoir si l'admission de la preuve serait susceptible de déconsidérer l'administration de la justice. J'admets, comme M. Spencer et le ministère public intimé en conviennent, que nous pouvons trancher cette question sur la foi du dossier dont nous sommes saisis. Toutefois, je ne souscris pas à l'argument de M. Spencer selon lequel la preuve devrait être écartée. En effet, j'estime qu'il n'y a pas lieu qu'elle le soit.

[76] The test for applying s. 24(2) is set out in *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353. The court must "assess and balance the effect of admitting the evidence on society's confidence in the justice system having regard to: (1) the seriousness of the *Charter*-infringing state conduct . . ., (2) the impact of the breach on the *Charter*-protected interests of the accused . . ., and (3) society's interest in the adjudication of the case on its merits": para. 71.

[77] Turning first to the seriousness of the state conduct, my view is that it cannot be characterized as constituting either "[w]ilful or flagrant disregard of the *Charter*": *Grant*, at para. 75. Det. Sgt. Parisien testified that he believed the request to Shaw was authorized by law and that Shaw could consent to provide the information to him. He also testified, however, that he was aware that there were decisions both ways on the issue of whether this was a legally acceptable practice. While I would not want to be understood to be encouraging the police to act without warrants in "gray areas", in light of the fact that the trial judge and three judges of the Court of Appeal concluded that Det. Sgt. Parisien had acted lawfully, his belief was clearly reasonable. In short, the police were acting by what they reasonably thought were lawful means to pursue an important law enforcement purpose. There is no challenge to any other aspect of the information to obtain the search warrant. The nature of the police conduct in this case would not tend to bring the administration of justice into disrepute.

[78] The second *Grant* factor is the impact of the *Charter*-infringing conduct on Mr. Spencer's *Charter*-protected interests. That impact here was serious. As discussed above, anonymity is an important safeguard for privacy interests online. The violation of that anonymity exposed personal choices made by Mr. Spencer to be his own and subjected them to police scrutiny as such. This weighs in favour of excluding the evidence.

[76] Le critère relatif à l'application du par. 24(2) est énoncé dans l'arrêt *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353. Le tribunal doit « évaluer et mettre en balance l'effet que l'utilisation des éléments de preuve aurait sur la confiance de la société envers le système de justice en tenant compte de : (1) la gravité de la conduite attentatoire de l'État [. . .], (2) l'incidence de la violation sur les droits de l'accusé garantis par la *Charte* [. . .] et (3) l'intérêt de la société à ce que l'affaire soit jugée au fond » : par. 71.

[77] En ce qui concerne la gravité de la conduite de l'État, j'estime qu'il n'y a pas lieu de qualifier cette dernière de « non-respect délibéré ou manifeste de la *Charte* » : *Grant*, par. 75. Le sergent-détective Parisien a déclaré qu'il croyait que la demande adressée à Shaw était autorisée par la loi et que Shaw consentirait à lui fournir l'information. Il a toutefois ajouté qu'il connaissait l'existence de décisions contradictoires quant à la question de savoir si cette pratique était légale. Bien que je ne voudrais pas qu'on comprenne des présents motifs que j'encourage les policiers à agir sans mandat dans les « zones grises », vu que le juge du procès et les trois juges de la Cour d'appel ont conclu que le sergent-détective Parisien avait agi légalement, sa conviction était manifestement raisonnable. Bref, les policiers se sont servi de ce qu'ils croyaient raisonnablement être des moyens légitimes pour poursuivre un objectif important visant l'application de la loi. Les autres aspects relatifs à la dénonciation justifiant l'obtention du mandat de perquisition ne sont pas contestés. Par sa nature, la conduite des policiers en l'espèce ne serait pas susceptible de déconsidérer l'administration de la justice.

[78] Le deuxième facteur énoncé dans l'arrêt *Grant* porte sur l'incidence de la conduite attentatoire sur les droits de M. Spencer garantis par la *Charte*. L'incidence était très grave en l'espèce. Rappelons que l'anonymat constitue une protection importante des droits en matière de vie privée à l'égard des activités en ligne. La violation de l'anonymat a exposé les choix personnels de M. Spencer et les a soumis à l'examen de la police. Ce facteur favorise l'exclusion de la preuve.

[79] That brings me to the final factor, society's interest in an adjudication on the merits. As explained in *Grant*,

> while the public has a heightened interest in seeing a determination on the merits where the offence charged is serious, it also has a vital interest in having a justice system that is above reproach, particularly where the penal stakes for the accused are high. [para. 84]

[80] The offences here are serious and carry minimum prison sentences. Society has both a strong interest in the adjudication of the case and also in ensuring that the justice system remains above reproach in its treatment of those charged with these serious offences. If the evidence is excluded, the Crown will effectively have no case. The impugned evidence (the electronic files containing child pornography) is reliable and was admitted by the defence at trial to constitute child pornography. Society undoubtedly has an interest in seeing a full and fair trial based on reliable evidence, and all the more so for a crime which implicates the safety of children.

[81] Balancing the three factors, my view is that exclusion of the evidence rather than its admission would bring the administration of justice into disrepute, and I would uphold its admission.

D. *The Fault Element of the "Making Available" Offence*

[82] The Court of Appeal ordered a new trial on the "making available" count on the basis that the trial judge had erred in his analysis of the fault requirement for the offence. It found that the trial judge had erred by finding that the making available offence required that Mr. Spencer knew that some positive act on his part facilitated access by others to the pornography. This error, in the Court of Appeal's view, led the judge to fail to consider whether Mr. Spencer had been wilfully blind to the fact that the pornography was being made available to others

[79] Je passe maintenant au dernier facteur, à savoir l'intérêt de la société à ce que l'affaire soit jugée au fond. Comme il est expliqué dans l'arrêt *Grant*,

> si la gravité d'une infraction accroît l'intérêt du public à ce qu'il y ait un jugement au fond, l'intérêt du public en l'irréprochabilité du système de justice n'est pas moins vital, particulièrement lorsque l'accusé encourt de lourdes conséquences pénales. [par. 84]

[80] Les infractions reprochées en l'espèce sont graves et sont punissables de peines minimales d'emprisonnement. La société a un intérêt manifeste à la fois à ce que l'affaire soit jugée et à ce que le fonctionnement du système de justice demeure irréprochable au regard des individus accusés de ces infractions graves. Si la preuve est écartée, le ministère public n'aura effectivement aucun recours à faire valoir. Les éléments de preuve contestés (les fichiers électroniques contenant de la pornographie juvénile) sont fiables et la défense a admis lors du procès qu'ils constituaient de la pornographie juvénile. La société a sans doute un intérêt à ce que l'affaire soit jugée dans le cadre d'un procès juste et équitable, fondé sur une preuve fiable, et encore plus dans le cas d'un crime qui vise la sécurité des enfants.

[81] Après avoir mis en balance les trois facteurs, j'estime que c'est l'exclusion de la preuve, et non son admission, qui serait susceptible de déconsidérer l'administration de la justice et je suis d'avis de confirmer l'admission de cette preuve.

D. *L'élément de faute de l'infraction de « rendre accessible »*

[82] La Cour d'appel a ordonné la tenue d'un nouveau procès sur le chef d'accusation de « rendre accessible », au motif que le juge du procès avait commis une erreur dans son analyse relative à l'exigence de faute de l'infraction. Selon la Cour, le juge du procès a commis une erreur en concluant que l'infraction de rendre accessible exigeait que M. Spencer ait connaissance que certaines de ses actions délibérées avaient facilité l'accès d'autres personnes à la pornographie. De l'avis de la Cour, le juge a ainsi omis de se demander si M. Spencer

through the shared folder. I respectfully agree with the Court of Appeal on both points and would affirm the order for a new trial.

[83] There is no dispute that the accused in a prosecution under s. 163.1(3) of the *Criminal Code* must be proved to have had knowledge that the pornographic material was being made available. This does not require, however, as the trial judge suggested, that the accused must knowingly, by some positive act, facilitate the availability of the material. I accept Caldwell J.A.'s conclusion that the offence is complete once the accused knowingly makes pornography available to others. As he put it,

> [i]n the context of a file sharing program, the *mens rea* element of making available child pornography under s. 163.1(3) requires proof of the intent to make computer files containing child pornography available to others using that program or actual knowledge that the file sharing program makes files available to others. [para. 87]

While the trial judge's reasons may perhaps be open to more than one interpretation on this point, reading his reasons as a whole, I also agree with Caldwell J.A. that the trial judge erred in deciding that a positive act was required to satisfy the *mens rea* component of the making available offence: para. 81.

[84] I further agree with Caldwell J.A. that wilful blindness was a live issue on the evidence and that it was because of the trial judge's error in relation to positive facilitation that he did not turn his mind to the evidence that could support an inference of wilful blindness. Wilful blindness is a substitute for knowledge. As explained by Charron J. in *R. v. Briscoe*, 2010 SCC 13, [2010] 1 S.C.R. 411, at para. 21,

avait fait preuve d'aveuglement volontaire quant à l'accessibilité de la pornographie à d'autres personnes au moyen du répertoire partagé. Je souscris à l'opinion de la Cour d'appel sur ces deux points et je suis d'avis de confirmer l'ordonnance prescrivant la tenue d'un nouveau procès.

[83] Il n'est pas contesté que, dans le cadre d'une poursuite sous le régime du par. 163.1(3) du *Code criminel*, il faut prouver que l'accusé avait connaissance du fait que le matériel pornographique était rendu accessible à d'autres personnes. Il n'est toutefois pas nécessaire, comme l'a suggéré le juge du procès, que l'accusé doive sciemment, par une certaine action concrète, faciliter l'accès au matériel. J'accepte la conclusion du juge Caldwell selon laquelle les éléments de l'infraction sont tous réunis lorsque l'accusé rend sciemment accessible la pornographie à d'autres personnes. Selon le juge :

> [TRADUCTION] S'agissant d'un programme de partage de fichiers, l'élément de *mens rea* relatif à l'infraction de rendre accessible de la pornographie juvénile prévue au par. 163.1(3) exige une preuve de l'intention de rendre les fichiers informatiques contenant de la pornographie juvénile accessibles à d'autres personnes en utilisant ce logiciel ou une connaissance réelle que le programme de partage de fichiers rend les fichiers accessibles à d'autres personnes. [par. 87]

Bien que les motifs formulés par le juge du procès se prêtent probablement à plusieurs interprétations sur ce point, compte tenu de leur ensemble, je partage également l'avis du juge Caldwell selon lequel le juge du procès a commis une erreur en décidant que la *mens rea* de l'infraction de rendre accessible exigeait l'accomplissement d'un geste délibéré : par. 81.

[84] À l'instar du juge Caldwell, j'estime aussi que l'aveuglement volontaire était une question en litige compte tenu de la preuve et qu'en raison de son erreur relative au geste délibéré le juge du procès ne s'est pas penché sur les éléments de preuve susceptibles d'étayer une conclusion d'aveuglement volontaire. L'aveuglement volontaire remplace la connaissance. Comme l'a expliqué la juge Charron dans l'arrêt *R. c. Briscoe*, 2010 CSC 13, [2010] 1 R.C.S. 411, par. 21 :

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

[85] The evidence calling for consideration of wilful blindness included, for example, evidence that in Mr. Spencer's statement to police he acknowledged the following: that LimeWire is a file-sharing program; that he had changed at least one default setting in LimeWire; that when LimeWire is first installed on a computer, it displays information notifying the user that it is a file-sharing program; that at the start of each session, LimeWire notifies the user that it is a file-sharing program and warns of the ramifications of file-sharing; and that LimeWire contains built-in visual indicators that show the progress of the uploading of files by others from the user's computer: paras. 88-89.

[86] Given that wilful blindness was a live issue and that the trial judge's error in holding that a positive act was required to meet the *mens rea* component of the making available offence resulted in his not considering the wilful blindness issue, I agree with Caldwell J.A. that the error could reasonably be thought to have had a bearing on his decision to acquit: para. 93; *R. v. Graveline*, 2006 SCC 16, [2006] 1 S.C.R. 609, at para. 14.

III. Disposition

[87] I would dismiss the appeal, affirm the conviction on the possession count and uphold the

L'ignorance volontaire ne définit pas la *mens rea* requise d'infractions particulières. Au contraire, elle peut remplacer la connaissance réelle chaque fois que la connaissance est un élément de la *mens rea*. La doctrine de l'ignorance volontaire impute une connaissance à l'accusé qui a des doutes au point de vouloir se renseigner davantage, mais qui choisit délibérément de ne pas le faire. Voir *Sansregret c. La Reine*, [1985] 1 R.C.S. 570, et *R. c. Jorgensen*, [1995] 4 R.C.S. 55. Comme l'a dit succinctement le juge Sopinka dans *Jorgensen* (par. 103), « [p]our conclure à l'ignorance volontaire, il faut répondre par l'affirmative à la question suivante : L'accusé a-t-il fermé les yeux parce qu'il savait ou soupçonnait fortement que s'il regardait, il saurait? » [Je souligne.]

[85] Parmi les éléments de preuve commandant l'examen de la question de l'aveuglement volontaire, mentionnons entre autres le fait que M. Spencer a reconnu dans sa déclaration à la police ceci : que LimeWire est un programme de partage de fichiers; qu'il avait modifié au moins un réglage par défaut de ce logiciel; que, lorsqu'il est installé la première fois sur un ordinateur, LimeWire affiche un message d'avertissement pour aviser l'utilisateur qu'il s'agit d'un programme de partage de fichiers; que, au début de chaque session, LimeWire avise l'utilisateur que c'est un programme de partage de fichiers et le met en garde contre les répercussions du partage de fichiers; que LimeWire contient des indicateurs visuels qui montrent la progression du téléchargement des fichiers par d'autres personnes à partir de l'ordinateur de l'utilisateur : par. 88-89.

[86] Puisque l'aveuglement volontaire était une question en litige et que l'erreur du juge du procès — lorsqu'il a conclu qu'un geste délibéré était nécessaire pour satisfaire à l'exigence de la *mens rea* de l'infraction de rendre accessible — lui a fait omettre l'examen de cette question, je conviens avec le juge Caldwell qu'il serait raisonnable de penser que cette erreur a eu une incidence sur le verdict d'acquittement : par. 93; *R. c. Graveline*, 2006 CSC 16, [2006] 1 R.C.S. 609, par. 14.

III. Dispositif

[87] Je suis d'avis de rejeter le pourvoi, de confirmer la déclaration de culpabilité relative au chef

Court of Appeal's order for a new trial on the making available count.

d'accusation de possession ainsi que l'ordonnance de Cour d'appel enjoignant la tenue d'un nouveau procès sur le chef d'accusation de rendre accessible.

APPENDIX

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

7. . . .

(3) [Disclosure without knowledge or consent] For the purpose of clause 4.3 of Schedule 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*) 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

. . .

(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

. . .

(*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

ANNEXE

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5

7. . . .

(3) [Communication à l'insu de l'intéressé et sans son consentement] 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 :

. . .

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 :

. . .

(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,

. . .

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

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;

. . .

Criminal Code, R.S.C. 1985, c. C-46

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.

. . .

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.

Appeal dismissed.

Solicitors for the appellant: McDougall Gauley, Regina.

Solicitor for the respondent: Attorney General for Saskatchewan, Regina.

Solicitor for the intervener the Director of Public Prosecutions: Public Prosecution Service of Canada, Edmonton and Halifax.

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;

. . .

Code criminel, L.R.C. 1985, ch. C-46

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.

. . .

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.

Pourvoi rejeté.

Procureurs de l'appelant : McDougall Gauley, Regina.

Procureur de l'intimée : Procureur général de la Saskatchewan, Regina.

Procureur de l'intervenant le directeur des poursuites pénales : Service des poursuites pénales du Canada, Edmonton et Halifax.

Solicitor for the intervener the Attorney General of Ontario: Attorney General of Ontario, Toronto.

Solicitor for the intervener the Attorney General of Alberta: Attorney General of Alberta, Calgary.

Solicitors for the intervener the Privacy Commissioner of Canada: Osler, Hoskin & Harcourt, Toronto.

Solicitors for the intervener the Canadian Civil Liberties Association: Kapoor Barristers, Toronto.

Solicitors for the intervener the Criminal Lawyers' Association of Ontario: Dawe & Dineen, Toronto; Schreck Presser, Toronto.

Procureur de l'intervenant le procureur général de l'Ontario : Procureur général de l'Ontario, Toronto.

Procureur de l'intervenant le procureur général de l'Alberta : Procureur général de l'Alberta, Calgary.

Procureurs de l'intervenant le commissaire à la protection de la vie privée du Canada : Osler, Hoskin & Harcourt, Toronto.

Procureurs de l'intervenante l'Association canadienne des libertés civiles : Kapoor Barristers, Toronto.

Procureurs de l'intervenante Criminal Lawyers' Association of Ontario : Dawe & Dineen, Toronto; Schreck Presser, Toronto.