Her Majesty the Queen v. Ward

[Indexed as: R. v. Ward]

112 O.R. (3d) 321

2012 ONCA 660

Court of Appeal for Ontario,
Winkler C.J.O., Doherty and Goudge JJ.A.
October 2, 2012

Charter of Rights and Freedoms -- Search and seizure -- Reasonable expectation of privacy -- Police officers in course of child pornography investigation asking Internet service provider ("ISP") to voluntarily provide name and address of subscriber assigned IP addresses on three particular occasions -- Police having information that IP address used to access or download child pornography three times over three-week period -- Request made in accordance with s. 7(3)(c.1) of Personal Information Protection and Electronic Documents Act -- ISP providing information sought by police -- Police using information provided along with other information to obtain search warrant for accused's residence -- Accused having subjective expectation of privacy in information revealing his Internet activity -- Expectation not objectively reasonable in circumstances of this case and in light of terms of service agreement between ISP and accused -- ISP permitted to consider that information sought pertaining to investigation involving serious offences against vulnerable members of society committed using resources of ISP -- ISP not infringing customer's objectively reasonable expectation of privacy in limited disclosure of information -- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s.

7(3)(c.1).

Charter of Rights and Freedoms -- Search and seizure -- Search with warrant -- Sufficiency of information to obtain warrant -- Information to obtain ("ITO") setting out strong evidence from which it could be inferred that someone using accused's computer at his residence had accessed or downloaded child pornography ten months earlier -- Technical information in ITO and evidence based on affiant's first-hand experience providing basis upon which justice could reasonably conclude that child pornography was still on computer and could be retrieved by police even if efforts having been made to delete it -- ITO containing sufficient grounds upon which search warrant for accused's residence could be issued.

The accused was charged with accessing and possessing child pornography. The owner of a German website filed a criminal complaint with the German police alleging that the website was being used to exchange child pornography files. The German authorities forwarded a list of IP addresses and the times and dates associated with the accessing of child pornography, along with copies of the related pornography, to the RCMP. In accordance with s. 7(3)(c.1) of the Personal Information Protection and Electronic Documents Act ("PIPEDA"), the RCMP sent letters of request to an Internet service provider asking for the name and address of the subscriber assigned three of those IP addresses at particular times. The ISP voluntarily provided the RCMP with the accused's name and address. The police used that information, along with other information, to obtain a search warrant for the accused's residence. They seized the accused's computers, which contained a large volume of child pornography. Following an unsuccessful application to exclude the evidence of the child [page322] pornography under s. 24(2) of the Canadian Charter of Rights and Freedoms, the accused was convicted. He appealed.

Held, the appeal should be dismissed.

It casts the question too narrowly to ask whether the accused had a subjective expectation of privacy that the ISP would not provide the police with his name and address. The information

provided by the ISP assisted the police in determining that someone in his house used the Internet to access and/or download child pornography at instants in times over a period of approximately three weeks. The accused had a subjective expectation of privacy in information revealing his Internet activity. However, that expectation was not objectively reasonable. There was nothing inherently confidential in the relationship between the accused and his ISP. The ISP was not acting as an agent of the police when it voluntarily complied with the police request. It was not compelled by any statute to provide the information to the police. It chose to do so when faced with a very specific and narrow request and when made aware of the nature of the investigation. The ISP had a legitimate interest in preventing the criminal misuse of its services, particularly in circumstances where the misuse effectively constituted the actus reus of a crime and involved an allegation of a serious offence committed against vulnerable members of society. A reasonable and informed person considering whether society would find it reasonable for the accused to have a reasonable expectation of privacy in his subscriber information would take into account the ISP's legitimate interests in voluntarily disclosing that information to the police when that disclosure would assist in the investigation of the alleged criminal misuse of its services, assuming the disclosure was not prohibited and would not violate any laws or the terms of the applicable customer agreement. The requests in this case complied with s. 7(3)(c.1) of PIPEDA. The police sought only the client's name and address. That information in and of itself revealed nothing personal about the accused or his Internet usage. The request was also narrow in the sense that it identified three specific instances of Internet activity. By disclosing the subscriber information to the police, the ISP would not be telling the police anything about the client's Internet activities at any time other than the three times identified in the requests. The service agreement between the ISP and the accused spoke of the ISP's willingness to disclose information in relation to investigations involving the alleged criminal misuse of its services. In particular, the accepted use policy made it clear that uploading or downloading child pornography was a breach of the accepted use policy and that the ISP would co-operate with

law enforcement agencies in connection with any investigation arising from a breach of the AUP.

The information to obtain the search warrant contained sufficient grounds upon which a search warrant could have issued. It provided strong evidence from which it could be inferred that someone using the accused's computer at his residence had accessed or downloaded child pornography ten months earlier on three occasions over a period of about three weeks. The information to obtain also provided extensive technical evidence to the effect that files downloaded by the accused on the computer could be recovered by police technicians even if the accused had tried to delete those files. Finally, the affiant provided detained evidence, based on his first-hand experiences, that individuals who access and possess child pornography on their computers often kept the images for long periods of time and rarely deleted collections. The technical evidence and the affiant's opinion evidence provided a basis upon which the justice could reasonably infer that there was a reasonable probability that the child pornography was still on the computer and could be retrieved by the police. [page323]

Cases referred to

R. v. Gomboc, [2010] 3 S.C.R. 211, [2010] S.C.J. No. 55, 2010 SCC 55, 221 C.R.R. (2d) 198, 2010EXP-3806, 34 Alta. L.R. (5th) 1, 408 N.R. 1, J.E. 2010-2060, EYB 2010-182517, 490 A.R. 327, 263 C.C.C. (3d) 383, 92 W.C.B. (2d) 36, 328 D.L.R. (4th) 71, [2011] 2 W.W.R. 442, 89 C.P.R. (4th) 199; R. v. Tessling, [2004] 3 S.C.R. 432, [2004] S.C.J. No. 63, 2004 SCC 67, 244 D.L.R. (4th) 541, 326 N.R. 228, J.E. 2004-2035, 192 O.A.C. 168, 189 C.C.C. (3d) 129, 23 C.R. (6th) 207, 123 C.R.R. (2d) 257, 62 W.C.B. (2d) 525; R. v. Trapp, [2011] S.J. No. 728, 2011 SKCA 143, 377 Sask. R. 246, [2012] 4 W.W.R. 648; R. v. Wise, [1992] 1 S.C.R. 527, [1992] S.C.J. No. 16, 133 N.R. 161, J.E. 92-354, 51 O.A.C. 351, 70 C.C.C. (3d) 193, 11 C.R. (4th) 253, 8 C.R.R. (2d) 53, 15 W.C.B. (2d) 158, consd

R. v. Morelli, [2010] 1 S.C.R. 253, [2010] S.C.J. No. 8, 2010 SCC 8, 207 C.R.R. (2d) 153, 399 N.R. 200, EYB 2010-171050, 2010EXP-1068, J.E. 2010-576, 252 C.C.C. (3d) 273, 316 D.L.R. (4th) 1, [2010] 4 W.W.R. 193, 72 C.R. (6th) 208, 346 Sask.

R. 1, 86 W.C.B. (2d) 949, distd

Other cases referred to

Hunter v. Southam Inc., [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36, 11 D.L.R. (4th) 641, 55 N.R. 241, [1984] 6 W.W.R. 577, J.E. 84-770, 33 Alta. L.R. (2d) 193, 55 A.R. 291, 27 B.L.R. 297, 14 C.C.C. (3d) 97, 2 C.P.R. (3d) 1, 41 C.R. (3d) 97, 9 C.R.R. 355, 84 D.T.C. 6467; R. v. Brousseau, [2010] O.J. No. 5793, 2010 ONSC 6753, 264 C.C.C. (3d) 562 (S.C.J.); R. v. Buhay, [2003] 1 S.C.R. 631, [2003] S.C.J. No. 30, 2003 SCC 30, 225 D.L.R. (4th) 624, 305 N.R. 158, [2004] 4 W.W.R. 1, J.E. 2003-1124, 177 Man. R. (2d) 72, 174 C.C.C. (3d) 97, 10 C.R. (6th) 205, 122 A.C.W.S. (3d) 863, 57 W.C.B. (2d) 206; R. v. Colarusso, [1994] 1 S.C.R. 20, [1994] S.C.J. No. 2, 110 D.L.R. (4th) 297, 162 N.R. 321, J.E. 94-240, 69 O.A.C. 81, 87 C.C.C. (3d) 193, 26 C.R. (4th) 289, 19 C.R.R. (2d) 193, 49 M.V.R. (2d) 161, 22 W.C.B. (2d) 154; R. v. Cole (2011), 105 O.R. (3d) 253, [2011] O.J. No. 1213, 2011 ONCA 218, 231 C.R.R. (2d) 76, 277 O.A.C. 50, [2011] CLLC 210-018, 269 C.C.C. (3d) 402, 90 C.C.E.L. (3d) 1, 83 C.R. (6th) 1, 94 W.C.B. (2d) 137; R. v. Cuttell, [2009] O.J. No. 4053, 2009 ONCJ 471, 201 C.R.R. (2d) 342, 247 C.C.C. (3d) 424; R. v. D'Amour, [2002] O.J. No. 3103, 163 O.A.C. 164, 166 C.C.C. (3d) 477, 4 C.R. (6th) 275, 96 C.R.R. (2d) 315, 55 W.C.B. (2d) 116 (C.A.); R. v. Duarte (1990), 71 O.R. (2d) 575, [1990] 1 S.C.R. 30, [1990] S.C.J. No. 2, 65 D.L.R. (4th) 240, 103 N.R. 86, J.E. 90-263, 37 O.A.C. 322, 53 C.C.C. (3d) 1, 74 C.R. (3d) 281, 45 C.R.R. 278, 9 W.C.B. (2d) 230; R. v. Dyment, [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, 55 D.L.R. (4th) 503, 89 N.R. 249, J.E. 89-77, 73 Nfld. & P.E.I.R. 13, 45 C.C.C. (3d) 244, 66 C.R. (3d) 348, 38 C.R.R. 301, 10 M.V.R. (2d) 1, 6 W.C.B. (2d) 78; R. v. Edwards (1996), 26 O.R. (3d) 736, [1996] 1 S.C.R. 128, [1996] S.C.J. No. 11, 132 D.L.R. (4th) 31, 192 N.R. 81, J.E. 96-349, 88 O.A.C. 321, 104 C.C.C. (3d) 136, 45 C.R. (4th) 307, 33 C.R.R. (2d) 226, 29 W.C.B. (2d) 366; R. v. Evans, [1996] 1 S.C.R. 8, [1996] S.C.J. No. 1, 131 D.L.R. (4th) 654, 191 N.R. 327, J.E. 96-254, 69 B.C.A.C. 81, 104 C.C.C. (3d) 23, 45 C.R. (4th) 210, 33 C.R.R. (2d) 248, 29 W.C.B. (2d) 276; R. v. Garofoli, [1990] 2 S.C.R. 1421, [1990] S.C.J. No. 115, 116 N.R. 241, J.E. 90-1684, 43 O.A.C. 1, 36 Q.A.C. 161, 60 C.C.C. (3d) 161, 80 C.R. (3d) 317, 50 C.R.R. 206, 11 W.C.B. (2d) 342; R. v.

Kang-Brown, [2008] 1 S.C.R. 456, [2008] S.C.J. No. 18, 2008 SCC 18, EYB 2008-132461, J.E. 2008-905, 77 W.C.B. (2d) 288, 230 C.C.C. (3d) 289, 87 Alta. L.R. (4th) 1, 373 N.R. 67, 55 C.R. (6th) 240, [2008] 6 W.W.R. 17, 293 D.L.R. (4th) 99, 432 A.R. 1, 169 C.R.R. (2d) 61; R. v. Kwok, [2008] O.J. No. 2414, 78 W.C.B. (2d) 21 (C.J.); R. v. Law, [2002] 1 S.C.R. 227, [2002] S.C.J. No. 10, 2002 SCC 10, 208 D.L.R. (4th) 207, 281 N.R. 267, J.E. 2002-325, 245 N.B.R. (2d) 270, 160 C.C.C. (3d) 449, 48 C.R. (5th) 199, 90 C.R.R. (2d) 55, 2002 D.T.C. 6789, [2002] G.S.T.C. 12, REJB 2002-27815, 52 W.C.B. (2d) 148; R. v. M. (A.) (2008), 92 O.R. (3d) 398, [2008] 1 S.C.R. 569, [2008] S.C.J. No. 19, 2008 SCC 19, EYB 2008-132460, J.E. 2008-904, 77 W.C.B. (2d) 289, 230 C.C.C. (3d) 377, 373 N.R. 198, 55 C.R. (6th) 314, 293 D.L.R. (4th) 187, 236 O.A.C. 267, 169 C.R.R. (2d) 1; [page324] R. v. McNeice, [2010] B.C.J. No. 2131, 2010 BCSC 1544; R. v. Nolet, [2010] 1 S.C.R. 851, [2010] S.C.J. No. 24, 2010 SCC 24, 213 C.R.R. (2d) 52, 76 C.R. (6th) 1, 403 N.R. 1, 320 D.L.R. (4th) 1, 95 M.V.R. (5th) 1, EYB 2010-175730, 2010EXP-2088, 256 C.C.C. (3d) 1, J.E. 2010-1151, 350 Sask. R. 51, [2010] 8 W.W.R. 1; R. v. Patrick, [2009] 1 S.C.R. 579, [2009] S.C.J. No. 17, 2009 SCC 17, 387 N.R. 44, J.E. 2009-665, 242 C.C.C. (3d) 158, 304 D.L.R. (4th) 260, 64 C.R. (6th) 1, 4 Alta. L.R. (5th) 1, [2009] 5 W.W.R. 387, 454 A.R. 1, EYB 2009-157141; R. v. Plant, [1993] 3 S.C.R. 281, [1993] S.C.J. No. 97, 157 N.R. 321, [1993] 8 W.W.R. 287, J.E. 93-1673, 12 Alta. L.R. (3d) 305, 145 A.R. 104, 84 C.C.C. (3d) 203, 24 C.R. (4th) 47, 17 C.R.R. (2d) 297, 20 W.C.B. (2d) 591; R. v. Spencer, [2011] S.J. No. 729, 2011 SKCA 144, 377 Sask. R. 280, [2012] 4 W.W.R. 425, 283 C.C.C. (3d) 384, 99 W.C.B. (2d) 210; R. v. Vasic, [2009] O.J. No. 685, 185 C.R.R. (2d) 286 (S.C.J.); R. v. Ward, [2008] O.J. No. 3116, 2008 ONCJ 355, 176 C.R.R. (2d) 90, 79 W.C.B. (2d) 129; R. v. Wilson, [2009] O.J. No. 1067, 2009 CarswellOnt 2064 (S.C.J.); R. v. Wong, [1990] 3 S.C.R. 36, [1990] S.C.J. No. 118, 120 N.R. 34, J.E. 90-1682, 45 O.A.C. 250, 60 C.C.C. (3d) 460, 1 C.R. (4th) 1, 2 C.R.R. (2d) 277, 11 W.C.B. (2d) 350; Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979); Thomson Newspapers Ltd. v. Canada, [1990] 1 S.C.R. 425, [1990] S.C.J. No. 23, 67 D.L.R. (4th) 161, 106 N.R. 161, J.E. 90-575, 39 O.A.C. 161, 54 C.C.C. (3d)

417, 29 C.P.R. (3d) 97, 76 C.R. (3d) 129, 47 C.R.R. 1; United States of America v. Bynum, 604 F. 3d 161 (4th Cir. 2010); United States of America v. Perrine, 518 F. 3d 1196 (10th Cir. 1998); United States v. Jones, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012); United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976); Warman v. Wilkins-Fournier (2010), 100 O.R. (3d) 648, [2010] O.J. No. 1846, 2010 ONSC 2126, 261 O.A.C. 245, 319 D.L.R. (4th) 268, 95 C.P.C. (6th) 385 (Div. Ct.)

Statutes referred to

Canadian Charter of Rights and Freedoms, ss. 8, 24(2)

Criminal Code, R.S.C. 1985, c. C-46, s. 487.014(1), 487.02(1)

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 2 [as am.], 3, 4, 5(1), (3), 7(3) [as am.], (c.1), (ii), Sch. 1

Royal Canadian Mounted Police Act, R.S.C. 1985, c. R-10 [as am.]

Authorities referred to

Hubbard, Robert W., Peter DeFreitas and Susan Magotiaux, "The Internet -- Expectations of Privacy in a New Context" (2001), 45 Crim. L.Q. 170

Morin, Suzanne, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", Privacy Pages: CBA National and Privacy Access Law Section Newsletter (November 2011)

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

Stringham, James A.Q., "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core of Section 8?" (2005), 23 C.R. (6th) 245

Westin, Alan F., Privacy and Freedom (New York: Athenum, 1967)

APPEAL by the accused from the conviction entered by Lalande J., [2008] O.J. No. 3116, 2008 ONCJ 355.

Jonathan Dawe, for appellant.

Michal Fairburn, for respondent. [page325]

James Stribopoulos and Lindsay Daviau, for intervenor Canadian Civil Liberties Association.

The judgment of the court was delivered by

DOHERTY J.A.: --

I

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

[2] The police, in the course of investigating child pornography crimes on the Internet, sometimes request and receive the names and addresses of customers from Internet service providers ("ISP"). The police make this request following a protocol developed by the police and the ISPs, but without seeking or obtaining any prior judicial authorization. Using information gathered from other sources and the information provided by the ISP, the police can connect a customer's account to specific Internet activity. That connection may assist in developing reasonable and probable grounds to obtain a search warrant for the customer's residence and computer. Those searches may in turn lead to the discovery of child pornography, and the arrest and prosecution of the customer for child pornography offences.

[3] The police practice of seeking and obtaining customer information from ISPs and using that information to obtain search warrants has been constitutionally challenged as an unreasonable search and seizure in several cases. The majority of the cases have held that a customer does not have a reasonable expectation of privacy in the information provided by the ISP: e.g., see R. v. Trapp, [2011] S.J. No. 728, 2011 SKCA 143, 377 Sask. R. 246, Ottenbreit J.A., concurring; R. v.

Spencer, [2011] S.J. No. 729, 2011 SKCA 144, 377 Sask. R. 280, Caldwell J.A., concurring; R. v. Wilson, [2009] O.J. No. 1067, 2009 CarswellOnt 2064 (S.C.J.); R. v. Vasic, [2009] O.J. No. 685, 185 C.R.R. (2d) 286 (S.C.J.); R. v. Brousseau, [2010] O.J. No. 5793, 2010 ONSC 6753, 264 C.C.C. (3d) 562 (S.C.J.); and R. v. McNeice, [2010] B.C.J. No. 2131, 2010 BCSC 1544. Others have recognized a reasonable expectation of privacy in the information, but have held that the police acted reasonably in obtaining the information without prior judicial authorization: see Trapp, Cameron J.A., for the majority. Some cases have [page326] found a violation of s. 8 of the Canadian Charter of Rights and Freedoms: e.g., see R. v. Kwok, [2008] O.J. No. 2414, 78 W.C.B. (2d) 21 (C.J.); R. v. Cuttell, [2009] O.J. No. 4053, 2009 ONCJ 471, 247 C.C.C. (3d) 424. This court addresses the constitutionality of this police practice for the first time. I would hold that in the circumstances presented here, the appellant has not established a reasonable expectation of privacy.

II

Overview and Position of the Parties

[4] The police, in the course of a child pornography investigation, sought the name and address of a customer (sometimes referred to as subscriber information) from Bell Sympatico, a Canadian ISP. Bell Sympatico chose to co-operate with the police and provided what turned out to be the appellant's name and address. That information, combined with other information gathered by the police during their investigation, enabled the police to obtain a search warrant for the appellant's residence and his computer. That search yielded over 30,000 images of child pornography, along with about 373 videos containing child pornography. The appellant was charged with one count of possession of child pornography and one count of accessing child pornography.

[5] At trial, the appellant defended the charges exclusively on the basis that the search of his residence and computer violated his rights under s. 8 of the Charter, and that s. 24(2) of the Charter required the exclusion of the evidence found in the search. The trial judge rejected the Charter claim and admitted the evidence: R. v. Ward, [2008] O.J. No. 3116,

2008 ONCJ 355, 176 C.R.R. (2d) 90. Convictions followed and the appellant was sentenced to 11 months' imprisonment and three years' probation. He appealed his convictions and sentences, but has abandoned his sentence appeal.

[6] The appellant raises two grounds of appeal. Both repeat the arguments unsuccessfully advanced at trial. First, the appellant submits that he had a reasonable expectation of privacy in his subscriber information held by Bell Sympatico and that his constitutional right to be free from unreasonable search and seizure was violated when Bell Sympatico, at the request of the police, turned that information over to the police. The appellant contends that the police acted unconstitutionally in requesting and obtaining that information without prior judicial authorization, other lawful authority, the appellant's consent or exigent circumstances. [page327]

[7] The appellant further submits that the information obtained through the unconstitutional seizure of his subscriber information was used to obtain the search warrant for his residence and computer and that without the subscriber information the police could not have obtained the warrant. It follows, the appellant argues, that if the subscriber information was obtained unconstitutionally, the search warrant is invalid, rendering the search of the appellant's residence and seizure of his computer unlawful and contrary to s. 8.

[8] Finally, the appellant contends that the fruits of the search should have been excluded under s. 24(2). As it is common ground that without the seized evidence the Crown had no case, the appellant asks the court to quash the convictions and enter acquittals.

[9] The appellant's second argument focuses on the adequacy of the contents of the information sworn to obtain the search warrant ("ITO") and assumes that the police had lawfully obtained the appellant's subscriber information from Bell Sympatico. The appellant submits that the totality of the evidence relied on in the ITO did not provide grounds upon which a justice of the peace, acting judicially, could issue a search warrant. As with the first ground of appeal, the

appellant contends that if this argument succeeds, the search and seizure violate s. 8, the evidence should be excluded under s. 24(2) and acquittals must follow.

[10] The Crown responds that the trial judge correctly found that the appellant had no reasonable expectation of privacy in respect of his subscriber information held by Bell Sympatico. Absent a reasonable expectation of privacy, there could be no breach of the appellant's rights under s. 8 when the police acquired that information from Bell Sympatico. On the second issue, the Crown submits that on a review of the entirety of the ITO, there were ample grounds upon which the justice of the peace could, acting judicially, issue the warrant. Finally, the Crown argues that if either of the appellant's arguments succeeds, the fruits of the search of the appellant's residence and the seizure of his computer should not be excluded under s. 24(2) and the convictions should stand.

[11] The grounds of appeal do not require any discussion of the factual merits of the allegations. The exclusion of the evidence under s. 24(2) of the Charter was the appellant's only hope for acquittals. If the evidence was admissible, the appellant's guilt was established beyond any reasonable doubt. [page328]

III

Issue #1: Did the Appellant have a Reasonable Expectation of Privacy in the Subscriber Information

A. The trial judge's reasons

[12] The trial judge correctly recognized that the appellant could not successfully advance a s. 8 claim unless he could demonstrate that he had a reasonable expectation of privacy in respect of the subscriber information held by Bell Sympatico. The trial judge, again correctly, understood that in determining whether the appellant had demonstrated a reasonable expectation of privacy, he had to consider the totality of the circumstances, including whether the appellant had a subjective expectation of privacy in respect of that information: see R. v. Tessling, [2004] 3 S.C.R. 432, [2004] S.C.J. No. 63, 2004 SCC 67, at paras. 18-19; R. v. Patrick, [2009] 1 S.C.R. 579, [2009] S.C.J. No. 17, 2009 SCC 17, at paras. 26-27; and R.

v. Gomboc, [2010] 3 S.C.R. 211, [2010] S.C.J. No. 55, 2010 SCC 55, at para. 18, Deschamps J., concurring, at paras. 77-78, Abella J., concurring.

[13] The trial judge focused his analyses on three factors. First, he noted that the requests for assistance made by the RCMP and Bell Sympatico's co-operation with those requests conformed to the federal legislation governing disclosure of customer information to law enforcement by private sector organizations such as Bell Sympatico.

[14] Second, the trial judge referred, at some length, to the terms of the service agreement between the appellant and Bell Sympatico, and the documents related to that service agreement. That agreement addressed both Bell Sympatico's commitment to maintaining the confidentiality of client information and its willingness to disclose client information to law enforcement authorities in connection with criminal investigations involving allegations of the criminal misuse of Bell Sympatico's services.

[15] Lastly, the trial judge emphasized the nature of the information turned over to the RCMP by Bell Sympatico. In his view, that information, the appellant's name and address, was not the kind of information that would reveal intimate personal details or lifestyle choices. The trial judge concluded his analysis of the totality of the circumstances, at para. 68 of his reasons:

> [T]he name and address was in the hands of a third party. The third party was entitled to measure its obligation to maintain confidentiality over personal information in accordance with its contractual arrangement with the subscriber. Although the applicant had a subjective expectation of privacy, I [page329] find in looking at the totality of the evidence that there was no objective reasonable expectation of privacy. In other words the subjective expectation was not objectively reasonable having regard to all contextual factors and the totality of the circumstances.

[16] The trial judge's finding that the appellant had no reasonable expectation of privacy in the subscriber information decided the s. 8 claim against the appellant. The trial judge had no need to go on and consider the reasonableness of the police conduct in obtaining the information from Bell Sympatico.

B. The "totality of the circumstances" in this case

[17] As the trial judge's reasons demonstrate, the totality of the circumstances engaged in this case has technical, investigative, legislative and contractual components. I will examine each separately. In doing so, I have tried to remain within the four corners of the trial record, although counsel, in an effort to educate the court (or at least one member of the panel), did refer to some aspects of the operation of the Internet, which they agreed were common knowledge.

[18] I refer specifically to the need to stay within the evidentiary record, usually a self-evident proposition, because a review of other cases that have addressed this same issue suggests an understanding of the nature of an Internet protocol address ("IP address") that is different than that offered by the evidence in this case. Some cases indicate that the IP address is "unique to that subscriber", e.g., Kwok, at para. 8, and that armed with subscriber information and an IP address the police can compile a "history of [the subscriber's] activity on that network": Trapp, at para. 36, Cameron J.A., for the majority, at para. 78, Ottenbreit J.A., concurring. As outlined below, the evidence in this case does not support the contention that IP addresses are unique to individual subscribers or that combining an IP address with subscriber information allows the police to compile a history of a person's activity on the Internet. On this record, what is revealed is more in the nature of a snapshot than a history of one's Internet activity.

(i) The technical information

[19] The Internet, as a global system of computer networks, has become an increasingly important tool for the exchange of information. Internet use for a variety of reasons is ubiquitous in today's society. In many ways, the Internet has

become the new library, shopping mall theatre, meeting hall and enumerable other venues all rolled into a single global venue available at the user's fingertips wherever he or she might be. [page330]

[20] Generally speaking, access to the Internet is provided to individual subscribers through an ISP. A subscriber connects to the ISP network which in turn connects the subscriber to the Internet. The subscriber pays a fee for that service. There are a number of Canadian ISPs, including Bell Sympatico.

[21] An IP address is a multi-digit numerical identifier that is automatically and randomly assigned by an ISP to a subscriber when the subscriber's computer device connects to the Internet. For example, one of the IP addresses identified on this appeal was 69.159.6.125. There are over 4.3 billion IP addresses worldwide. IP addresses are reused and are not unique to individual subscribers, although at any given point in time, an IP address will be assigned to a specific subscriber.

[22] IP addresses belong to an ISP and are controlled by that ISP. The service agreement between Bell Sympatico and the appellant reflects the nature of an IP address in these terms:

> Any IP address . . . is the property of Your Service Provider at all times, and may be changed or withdrawn at any time in the sole discretion of Your Service Provider.

[23] The ISP records the dates and times that its IP addresses are assigned to its subscribers. These records identify the subscribers' accounts on which the Internet was accessed at particular times. However, that does not necessarily mean that the subscriber himself or herself was using the computer connected to the Internet at that time, or that it was even the subscriber's computer that was connected to the Internet. A wired or wireless network may link multiple computers to a central device referred to as a shared access point. When more than one computer is accessing the Internet through a shared access point at the same time, there are additional technical issues that may arise. However, this case is not concerned with multiple computers sharing an access

point.

[24] IP addresses are usually assigned randomly and can be changed by the ISP at any time. An IP address is generally assigned by the ISP when a subscriber connects to the Internet. The same IP address may last for the duration of the Internet connection or it may change during the same connection. A subscriber will usually receive a new IP address each time he or she connects to the Internet. It is unlikely that a subscriber will be assigned the same IP address on two different connections to the Internet. However, subscribers who leave their computer or device connected to the Internet continually could use the Internet on separate occasions while retaining the same IP address.

[25] The dynamic nature of an IP address is demonstrated in the details of the requests for information made in this case. The [page331] police asked Bell Sympatico for the name and address of the subscriber associated with an IP address used on June 16, 2006 between 06:09:24 and 06:09:48, a span of 24 seconds. The other two requests relating to connections made on July 2 and July 6 referred only to a single point in time. The information requested could not, in and of itself, reveal to the police anything about the subscriber's computer activity before or after the three connections referred to in the requests.

[26] The IP address being used at any particular point in time to connect a computer or a wired or wireless network to specific content on the Internet can be determined in various ways. As happened in this case, some website operators record the IP addresses of users who access their site. Those operators might choose to share that information with the police. If the police have a specific IP address, they can, by accessing a website that is available to the public, identify the ISP that controls that IP address and a geographic location where it is being used. In this case, three IP addresses were identified as belonging to Bell Sympatico at Sudbury.

(ii) The investigation

[27] Carookee.com is a website that has operated out of

Germany since 2001. It offers online forums open to the general public on a wide variety of topics, such as politics and sports. Individuals can create their own forum or page, or they may use an existing forum to post messages and exchange information. The website includes about 25,000 pages. Persons who access the website can do so anonymously, by utilizing anonymous e-mail addresses.

[28] In July 2006, the owner of the website filed a criminal complaint with the German police alleging that some 28 pages on the website were being used to exchange child pornography files. German authorities investigated and found that there were child pornographic images on 17 of the pages on the website.

[29] The German authorities, by reference to the IP addresses provided to them by the owner of the website, determined that some of the child pornographic material was being accessed through Canadian ISPs. In August or September 2006, the German authorities forwarded a list of 229 IP addresses and the times and dates associated with the accessing of the child pornography to the RCMP, along with copies of the related child pornography. By accessing a public website, the RCMP determined that three of the IP addresses belonged to Bell Sympatico and were connected to the Sudbury area. The three IP addresses and the relevant times and dates of the Internet connections were [page332]

-- IP address 69.159.6.125 between 06:09:24 and 06:09:48 on June 16, 2006;

-- IP address 69.159.10.48 at 04:35:40 on July 2, 2006; and

-- IP address 69.159.7.45 at 06:06:04 on July 6, 2006.

[30] Access to the carookee.com site required a person to provide an e-mail address. The three connections described above had been made using temporary e-mail addresses obtained anonymously.

[31] On November 22, 2006, the RCMP sent letters of request

to Bell Sympatico asking for the subscriber information of the subscriber assigned the three IP addresses at the times set out above. The request indicated that it was being sent "in accordance with s. 7(3)(c.1) of the Personal Information Protection and Electronic Documents Act", S.C. 2000, c. 5 ("PIPEDA"). I will discuss that request in more detail below.

[32] Bell Sympatico chose to comply with the requests. Bell Sympatico provided the name and address of the subscriber -- the appellant, David Ward. It did not provide any other information.

[33] After receiving the subscriber information, the RCMP contacted the Sudbury Police. Detective Constable Burtt took carriage of the investigation for that force. He viewed the images that had been provided to the RCMP by the German authorities. The first incident, on June 16, 2006, involved the accessing of six images, each depicting a prepubescent boy with an erect penis. The second and third incidents, on July 2 and July 6, 2006, involved the downloading of an image of a prepubescent boy with an erect penis. The same image was downloaded on both dates. Detective Constable Burtt was satisfied that all of the images accessed on the three dates fell within the legal definition of child pornography.

[34] Detective Constable Burtt and others on the Sudbury Police force conducted further investigations. Several sources confirmed that the appellant lived at the residence. Another officer was also able to confirm that the appellant lived alone, had a computer, did not employ a wireless network and was a customer of Bell Sympatico. Armed with this information, the information provided by the German authorities, knowledge of the nature of the images and the subscriber information provided by Bell Sympatico, the Sudbury Police applied for a search warrant.

[35] On May 23, 2007, the Sudbury Police obtained a warrant to search the appellant's residence. They executed the warrant [page333] the next day, while the appellant was home alone. When the police entered the house, they saw child pornography

on the appellant's computer screen. The police seized four computers and related material. Forensic analysis revealed over 30,000 images and 373 videos of child pornography.

(iii) The legislative context: PIPEDA and the Criminal Code

[36] Several Canadian ISPs, including Bell Sympatico, have developed a protocol in conjunction with various Canadian law enforcement agencies to be used when those agencies are seeking subscriber information associated with the use of a specified IP address at a specific date and time. The protocol applies to child sexual exploitation investigations: see Suzanne Morin, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", Privacy Pages: CBA National and Privacy Access Law Section Newsletter (November 2011), pp. 1-20.

[37] Under the protocol, the police send a requesting letter to the ISP identifying the requesting officer, indicating that the officer is conducting an investigation in relation to child exploitation offences under the Criminal Code, R.S.C. 1985, c. C-46 and seeking disclosure of the last known customer name and address of an account holder associated with a specified IP address used at a specific date and time. The letter states that the request is made pursuant to s. 7(3)(c.1) of PIPEDA. The officer identifies his authority for the request by reference to the legislation governing the particular police force and the common law police powers. The letter provides no details of the specific investigation.

[38] The requesting letter contains a space where the information sought by the police can be inserted by the ISP. If the ISP chooses to provide that information, it fills in the space and returns the letter to the requesting officer.

[39] In this case, Bell Sympatico received requests, referable to each of the three IP address connected to images of child pornography. These requests complied with the protocol. Bell Sympatico chose to co-operate with the requests, inserted the appellant's subscriber information in the letters and returned them to the RCMP.

[40] PIPEDA, the statutory authority referred to in the form letter, is federal legislation governing the collection, use and disclosure of customers' personal information in the private sector. PIPEDA applies to any "organization" -- a broadly defined term in the Act -- that collects, uses or discloses the "personal [page334] information" -- again a broadly defined term in the Act -- in the course of their commercial activities: PIPEDA, ss. 2 and 4. PIPEDA applies to Bell Sympatico's disclosure of its customers' personal information.

[41] PIPEDA recognizes and seeks to protect an individual's right to privacy in respect of personal information provided to organizations. At the same time, PIPEDA acknowledges that disclosure of that information by those organizations will in some circumstances be reasonable and appropriate. The dual rationale underlying the legislation is reflected in s. 3:

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

[42] Subsection 5(3) further confirms reasonableness as the touchstone of permissible disclosure of personal information under the Act:

> 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

[43] Subsection 5(1) of PIPEDA requires that an organization, like Bell Sympatico, comply with the obligations set out in Sch. 1 of the Act. That schedule details the "Principles Set Out in the National Standard of Canada Entitled Model Code for

the Protection of Personal Information, CAN/CSA-Q830-96". The principles found in Sch. 1 begin from the premise that an organization cannot disclose personal information obtained from a customer without the knowledge and consent of the customer. As s. 3 and s. 5(3) acknowledge, however, disclosure is appropriate in certain circumstances. Subsection 7(3) of the Act sets out circumstances in which an organization may, if it chooses to do so, disclose a customer's personal information without the customer's knowledge or consent. Some of the circumstances described in s. 7(3) contemplate disclosure to governmental authorities, including the police. For present purposes, the relevant disclosure provision is s. 7(3)(c.1)(ii):

> 7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if the disclosure is
>
> . . . . . [page335]
>
> (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[.]

(Emphasis added)

[44] In this case, the letters of request sent by the RCMP to Bell Sympatico identified the "government institution" making the request -- the RCMP; identified the "lawful authority" for the request -- the Royal Canadian Mounted Police Act, R.S.C. 1985, c. R-10, the Royal Canadian Mounted Police Regulations and the common law; and indicated that the disclosure was requested only for the purpose of an investigation in relation to child sexual exploitation offences under the Criminal Code, a "law of Canada".

[45] The disclosure contemplated by s. 7(3) is discretionary. The organization asked to make disclosure of customer records must exercise that discretion in accordance with the overarching principle enunciated in s. 5(3) of PIPEDA. The disclosure must be for purposes that "a reasonable person would consider are appropriate in the circumstances". In exercising that discretion, the organization is entitled to consider factors such as the nature of the investigation, and the nature of the information requested: see Andrea Slane 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, at pp. 496-98.

[46] The trial judge found, at para. 57 of his reasons, and the parties and the intervenor agree, that PIPEDA does not create any police search and seizure powers. I agree with this interpretation. PIPEDA sets out the circumstances in which organizations may lawfully choose to disclose personal customer information, which must normally be kept confidential, to third parties, including, in some circumstances, the police.

[47] Crown counsel acknowledges that nothing in PIPEDA empowers the state to interfere with an individual's rights under s. 8 of the Charter. It does not follow that because an organization can disclose information to the state under PIPEDA that an individual has no privacy interest as against the state in that information for the purposes of s. 8. The terms of PIPEDA are, however, relevant to the s. 8 analysis to the extent that they [page336] speak to the existence and scope of a reasonable expectation of privacy in respect of information in the hands of an organization operating under the auspices of PIPEDA.

[48] Subsection 487.014(1) of the Criminal Code is also germane given the disclosure regime established by PIPEDA:

> 487.014(1) For greater certainty, no production order is necessary for a peace 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.

[49] Subsection 487.014(1) seems to state the self-evident, perhaps explaining the opening phrase "for greater certainty". The section provides that where a person is not prohibited by law from disclosing information, the police may request disclosure of that information without prior judicial authorization. Read with PIPEDA, s. 487.014(1) allows the police, without obtaining prior judicial authorization, to ask an organization for information which that organization is lawfully entitled to disclose under PIPEDA.

[50] With respect to the contrary opinion reached by the majority in Trapp, at para. 66, I do not read s. 487.014(1) as creating or extending any police search or seizure power. The police request identified in the section, standing alone, is not a search or seizure. The request, coupled with the voluntary co-operation with the request by the third party holder of the information, may or may not be a search or seizure depending on whether a claimant can establish a reasonable expectation of privacy in the information as against the state. That determination will depend on an assessment of the totality of the circumstances. Legislative provisions affecting either the police authority to request the information from third parties, e.g., s. 487.02(1), or the third party's ability to voluntarily disclose that information to the police, e.g., PIPEDA, are relevant to the reasonable expectation of privacy inquiry but do not create police powers to search or seize.

[51] The appellant does not challenge the constitutionality of either PIPEDA or s. 487.014(1).

(iv) The service agreement

[52] The relationship between Bell Sympatico and the appellant was governed by a service agreement and related documents setting out the terms on which Bell Sympatico agreed to provide services, including Internet connection, to the appellant. The contract between Bell Sympatico and the

appellant is a classic contract of adhesion. Bell Sympatico unilaterally set the terms of the service agreement and related documents. If the [page337] appellant wanted the service provided by Bell Sympatico, he had to agree to Bell Sympatico's terms.

[53] The terms of the service agreement included the following:

> You will not use the Service in a manner that is contrary to any applicable law or regulation, and you will abide by Your Service Provider's policies, including without limitation the Acceptable Use Policy, which set forth additional rules that govern your activity in connection with the Service.

[54] The acceptable use policy ("AUP") attached to the service agreement provided that any violation of the AUP constituted a violation of the service agreement that could result in termination of the agreement. The AUP specifically prohibited:

> 5. Uploading or downloading, transmitting, posting, publishing, disseminating, receiving, retrieving, storing or otherwise reproducing, distributing or providing access to information, software, files or other material which . . . (ii) are defamatory, obscene, child pornography or hate literature[.]
>
> . . . . .
>
> 11. Transmitting, posting, receiving, retrieving, storing or otherwise reproducing, distributing or providing access to any program or information constituting or encouraging conduct that would constitute a criminal offence[.]
>
> 12. Violating or breaching any applicable law[.]

(Emphasis added)

[55] Paragraph 17 of the service agreement put the appellant on notice that Bell Sympatico reserved the right

> . . . from time to time to monitor the Service electronically . . . and to disclose any information necessary to satisfy any laws, regulations or other governmental request from any

applicable jurisdiction, or as necessary to operate the Service or to protect itself or others.
(Emphasis added)

[56] In the AUP, Bell Sympatico made it clear that it would

. . . offer full co-operation with law enforcement agencies in connection with any investigation arising from a breach of this AUP.
(Emphasis added)

[57] The service agreement also addressed the privacy features Bell Sympatico offered to its customers. In the agreement, Bell Sympatico undertook to protect its clients' "personal information" in a manner that was consistent with Bell Customer Privacy Policy and the Bell Code of Fair Information Practices. While it is not entirely clear, it would appear that the name and address of a customer, standing alone, would not qualify as "personal information" for the purposes of Bell's privacy policy and practices. [page338]

[58] The service agreement further provided that customers like the appellant, by subscribing to the service, consented to the collection, use and disclosure of their personal information as described in Bell Sympatico's policies and practices, unless the customer specifically withdrew that consent by completing an "opt-out form". There is no evidence that the appellant "opted out".

C. Legal Analysis

(i) A broad and purposive interpretation of s. 8

[59] Before examining the specific issues raised on this appeal, it is important to describe the jurisprudential landscape on which the issue raised by this ground of appeal must be resolved. I begin with the language of s. 8. It declares with eloquent simplicity that:

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

[60] Section 8 stands as "a shield against unjustified state

intrusions on personal privacy": R. v. Kang-Brown, [2008] 1 S.C.R. 456, [2008] S.C.J. No. 18, 2008 SCC 18, at para. 8. Section 8 recognizes and constitutionally protects every person's right to live his or her life free of government intrusion except to the extent that the intrusion is reasonable. Personal privacy, broadly construed, includes control over one's body and bodily substances (physical privacy), control over certain places such as one's residence (territorial privacy), and control over information about the person and/or his activities (informational privacy): Tessling, at paras. 20-24.

[61] The fundamental importance of personal privacy cannot be denied. Personal privacy is a prerequisite to individual liberty, security, self-fulfilment and autonomy. Personal privacy is also a precondition to the maintenance of a thriving democratic society: R. v. Dyment, [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, at pp. 427-28 S.C.R.; R. v. Wong, [1990] 3 S.C.R. 36, [1990] S.C.J. No. 118, at pp. 45-46 S.C.R.; R. v. Wise, [1992] 1 S.C.R. 527, [1992] S.C.J. No. 16, at p. 558 S.C.R., La Forest J. dissenting (but not on this point); R. v. Plant, [1993] 3 S.C.R. 281, [1993] S.C.J. No. 97, at pp. 292-93 S.C.R.; and Tessling, at paras. 12-16.

[62] Section 8, like all Charter rights, must be interpreted broadly so as to best achieve the purpose underlying the right. As set out above, the protection of personal privacy from unreasonable state intrusion is the primary purpose of s. 8: [page339] Hunter v. Southam Inc., [1984] 2 S.C.R. 145, [1984] S.C.J. No. 36, at pp. 158-59 S.C.R.; Dyment, at p. 253.

[63] The purposive and broad interpretation of s. 8 is evident in the jurisprudence of the Supreme Court of Canada. Several facets of that jurisprudence are germane to this case. To begin with, the concepts of search and seizure are not defined by reference to the nature of the state conduct in issue, but primarily by reference to the effect of that conduct on the reasonable expectation of privacy of those targeted by the conduct: R. v. Evans, [1996] 1 S.C.R. 8, [1996] S.C.J. No. 1, at para. 11; R. v. Buhay, [2003] 1 S.C.R. 631, [2003] S.C.J.

No. 30, 2003 SCC 30, at paras. 33-34; R. v. Law, [2002] 1 S.C.R. 227, [2002] S.C.J. No. 10, 2002 SCC 10, at para. 15; Wise, at p. 538 S.C.R.; Tessling, at para. 18; and Gomboc, at para. 77, Abella J., concurring.

[64] Thus, while from the police perspective, it could be said that they merely asked Bell Sympatico for its assistance and Bell Sympatico volunteered its co-operation, from the appellant's perspective, the police, through their request and Bell Sympatico's co-operation, acquired personal information about the appellant's computer use that the appellant claimed he was reasonably entitled to expect would not be made available to the police without some prior judicial authorization. If the appellant had a reasonable expectation of privacy with respect to the information, the police acquisition of that information falls within the meaning of "search and seizure" for the purposes of s. 8 even though the state conduct was in no way coercive and Bell Sympatico voluntarily turned over the information.

[65] A purposive reading of s. 8 also requires that the court identify the subject matter of the alleged search, not narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action. Thus, in Patrick, at para. 29, the court described the target of the search, not as the appellant's garbage bags left on the street, but rather as the appellant's personal information that could be gleaned from an examination of the contents of the garbage bags. In Kang-Brown, at para. 58, the court described the target of the search by the sniffer dog as the contents of the bag sniffed, and not merely the air surrounding the bag. Similarly, in Tessling and in Gomboc, the court characterized searches by reference to the information that could potentially be revealed about activities with the home and not simply as information about electricity or heat consumption within the home.

[66] The proper characterization of the subject matter of the state conduct is important in this case. Ms. Fairburn, for the [page340] Crown, drawing on the analysis of the trial judge

and that found in the concurring reasons of Ottenbreit J.A. in Trapp, at paras. 119-24 and 134, contends that the police acquired only the appellant's name and address, information that was readily available to the public and could not possibly be viewed as private or confidential by anyone. Ms. Fairburn further submits that the nature of the information obtained by the police from Bell Sympatico does not change because, when combined with information the police had obtained lawfully from other sources, it connects the appellant to certain Internet activity.

[67] With respect to Ms. Fairburn's submissions, delivered with her customary clarity, her description of the target of the state action as the appellant's name and address is akin to the suggestion that the air around the bag was the target of the search conducted by the sniffer dog in Kang-Brown. That characterization does not describe what the police were really after, or what the appellant claims was within his reasonable expectation of privacy.

[68] The police did not want the subscriber information so as to be able to identify the appellant as a customer of Bell Sympatico. That fact alone was of no value to the police. Nor does the appellant contend that he has a reasonable expectation of privacy with respect to the fact that he is a client of Bell Sympatico. The police wanted the information because they believed it could potentially identify the appellant as the person who had anonymously accessed child pornography on three separate occasions over the Internet. Translated into the content neutral language required for the purposes of s. 8, the police wanted the information because of what it could potentially tell them about the appellant's Internet activity on three occasions. They sought to connect an identity to certain activity: see Slane and Austin, at pp. 500-503.

[69] I agree with Mr. Dawe, counsel for the appellant, that the reasonable expectation of privacy inquiry must be framed in terms of whether the police could access information "capable of revealing details about the appellant's Internet activities". I cannot, however, go so far as Mr. Dawe, and counsel for the intervenor, who, relying on the comments of

Cameron J.A. in Trapp, at paras. 32-37, argue that the information sought by the police would provide "an electronic roadmap of the appellant's travels on the Internet". That description, while consistent with the language used in Trapp, at para. 36, goes beyond the evidentiary record in this case. Adapting the intervenor's metaphor to the evidence adduced here, I would say that the police sought information capable of putting the [page341] appellant at a specific place, at a specific time in the course of his travels on the Internet.

[70] The privacy claim advanced by the appellant raises a further important point about the scope of the privacy right protected by s. 8. The appellant is arguing that he had a reasonable expectation that he could access and use the Internet anonymously and that s. 8 protects him against state access to information in the hands of third parties that would allow the state to identify the appellant's activities on the Internet, unless the state can satisfy the reasonableness requirement of s. 8. The appellant in essence claims that his privacy rights under s. 8 protect his anonymity while engaged in certain activities, even activities in public venues.

[71] Personal privacy is about more than secrecy and confidentiality. Privacy is about being left alone by the state and not being liable to be called to account for anything and everything one does, says or thinks. Personal privacy 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.

[72] In Wise, at p. 538 S.C.R., the court recognized an individual's expectation of privacy while engaged in very public activity. The court held that continual state electronic monitoring of the movements of an individual's vehicle on public highways violated that person's reasonable expectation of privacy. I take the court to have held that in Canadian society people can reasonably expect that they can move about on public highways without being identified and continually monitored by the state. If the state chooses to engage in that kind of invasive conduct, it must be able to meet the

constitutional requirements of s. 8. Wise holds that while the public nature of the forum in which an activity occurs will affect the degree of privacy reasonably expected, the public nature of the forum does not eliminate all privacy claims.

[73] The concept of privacy underlying Wise is described by Professor Westin as "public privacy": Alan F. Westin, Privacy and Freedom (New York: Athenum, 1967), at p. 32. He explains the relationship between anonymity and personal privacy in these terms, at p. 31:

> The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of [page342] behaviour and role that would operate if he were known to those observing him. In this state the individual is able to merge into the "situational landscape." Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.

(Emphasis added)

[74] I think that s. 8 encompasses the concept of "public privacy" described above. [See Note 1 below] Surely, if the state could unilaterally, and without restraint, gather information to identify individuals engaged in public activities of interest to the state, individual freedom and with it meaningful participation in the democratic process would be curtailed. It is hardly surprising that constant unchecked state surveillance of those engaged in public activities is a feature of many dystopian novels.

[75] By going on the website carookee.com, the appellant engaged with others in a public forum that was open to literally anyone around the world. The appellant did so, however, anonymously. Anonymity "to some degree at least" is a

feature of much Internet activity: Warman v. Wilkins-Fournier (2010), 100 O.R. (3d) 648, [2010] O.J. No. 1846, 2010 ONSC 2126 (Div. Ct.), at para. 20. Depending on the totality of the circumstances, his anonymity may enjoy constitutional protection under s. 8.

[76] A purposive approach to s. 8 also dictates that personal privacy claims be measured as against the specific state conduct and the purpose for that conduct. Section 8 is not about protecting individual privacy at large or as between non-state actors. Section 8 focuses on personal privacy claims in relation to state intrusions said to infringe on that personal privacy: Gomboc, at para. 34, Deschamps J., concurring. Because the focus is on state intrusion and the purpose of the intrusion, Canadian jurisprudence has emphatically rejected the "risk" analysis featured in American Fourth Amendment jurisprudence: e.g., see R. v. Duarte (1990), 71 O.R. (2d) 575, [1990] 1 S.C.R. 30, [1990] S.C.J. No. 2, at p. 48 S.C.R.; Wong, at p. 45 S.C.R. According to that jurisprudence, voluntary disclosure to third parties defeats Fourth Amendment claims: e.g., see Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979), at pp. 743-44 U.S.; United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619 (1976), at pp. 442-43 U.S.; and Robert W. Hubbard, Peter DeFreitas and Susan Magotiaux, [page343] "The Internet -- Expectations of Privacy in a New Context" (2001), 45 Crim. L.Q. 170, at pp. 177-85. [See Note 2 below]

[77] Under the Canadian jurisprudence, a person, by allowing others into a zone of personal privacy, does not forfeit a claim that the state is excluded from that same zone of privacy. Nor does allowing a state actor within a zone of personal privacy for a specified purpose automatically foreclose a claim of privacy as against the state should it enter that same zone of privacy for another purpose: R. v. Colarusso, [1994] 1 S.C.R. 20, [1994] S.C.J. No. 2, at p. 55 S.C.R.; Law, at paras. 19-22; Thomson Newspapers Ltd. v. Canada, [1990] 1 S.C.R. 425, [1990] S.C.J. No. 23; Gomboc, at paras. 100-102, McLachlin C.J.C. and Fish J., dissenting (but not on this point); R. v. D'Amour, [2002] O.J. No. 3103, 166 C.C.C. (3d) 477 (C.A.), at para. 57; and R. v. Cole (2011), 105

O.R. (3d) 253, [2011] O.J. No. 1213, 2011 ONCA 218, at paras. 74-78. On the purposive interpretation of s. 8, it is no answer to the appellant's s. 8 claim to assert that because the appellant willingly surrendered the relevant information to Bell Sympatico, he assumed the risk that Bell Sympatico would share the information with the police.

[78] In holding that the risk that Bell Sympatico would share the information does not necessarily defeat a s. 8 claim, I do not suggest that the relationship between the appellant and Bell Sympatico, particularly as it related to any agreement concerning the disclosure of information, was not relevant to the appellant's privacy claim. I mean only to say that willing disclosure to third parties is not determinative of the existence of a legitimate privacy claim under s. 8.

(ii) Section 8 protects only reasonable expectations of privacy

[79] Despite the centrality of personal privacy to the relationship between the individual and the state under the Canadian [page344] constitution, personal privacy, like any other individual right, cannot be absolute in a democratic society. One's right to be left alone by the state must be balanced against other legitimate competing societal interests, including the need to effectively investigate crime: Hunter, at pp. 159-60 S.C.R.; Tessling, at paras. 17-18. In Hunter, Dickson J. described the balance in these terms [at p. 159 S.C.R.]:

> The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as a freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.

[Emphasis added; underlining in original]

[80] The s. 8 jurisprudence strikes the balance between individual privacy and competing state interests by constitutionally protecting only privacy claims that are founded on a reasonable expectation of privacy and by prohibiting only state intrusions upon reasonable expectations of privacy that are unreasonable: Tessling, at paras. 17-18.

[81] How then is one to determine whether a claimant has "a reasonable expectation of privacy"? In Tessling, at para. 42, Binnie J. observes that "[e]xpectation of privacy is a normative rather than a descriptive standard".

[82] By "normative", I understand Binnie J. to mean that in determining whether an individual enjoys a reasonable expectation of privacy, the court is making a value judgment more than a finding of fact in the traditional sense. When the court accepts the contention that a person has a reasonable expectation of privacy, the court is in reality declaring that the impugned state conduct has reached the point at which the values underlying contemporary Canadian society dictate that the state must respect the personal privacy of individuals unless it is able to constitutionally justify any interference with that personal privacy.

[83] The normative nature of the reasonable expectation of privacy inquiry has been underscored in several pronouncements from the Supreme Court of Canada beginning in Wong, at pp. 45-46 S.C.R., where La Forest J. described the inquiry in these terms:

> [W]hether, by the standards of privacy that persons can expect to enjoy in a free and democratic society, the agents of the state were bound to conform to the requirements of the Charter when effecting the intrusion in question. [page345]

[84] In Patrick, at para. 14, Binnie J. stressed the long-term consequences on personal privacy of the impugned state action in assessing the privacy claim:

> Privacy analysis is 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.

[85] Most recently in Gomboc, Deschamps J., at para. 34, in her concurring reasons, captured the normative nature of the inquiry in these terms:

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

[86] The courts have approached the reasonable expectation of privacy inquiry by asking whether the claimant had a subjective expectation of privacy and, if so, whether in all of the circumstances that expectation was reasonable: e.g., see R. v. Edwards (1996), 26 O.R. (3d) 736, [1996] 1 S.C.R. 128, [1996] S.C.J. No. 11, at para. 45; R. v. Nolet, [2010] 1 S.C.R. 851, [2010] S.C.J. No. 24, 2010 SCC 24, at para. 30. While both questions help to focus the inquiry on the specific facts of the case and the values underlying s. 8, neither question captures the entirety of the reasonable expectation of privacy inquiry. Section 8 is concerned with the degree of privacy needed to maintain a free and open society, not necessarily the degree of privacy expected by the individual or respected by the state in a given situation. As Binnie J. put it in R. v. M. (A.) (2008), 92 O.R. (3d) 398, [2008] 1 S.C.R. 569, [2008] S.C.J. No. 19, 2008 SCC 19, at para. 33, s. 8 protects the privacy interests that

> . . . the citizen subjectively believes ought to be respected by the government and "that society is prepared to recognize as 'reasonable'"[.]

(Emphasis added; citation omitted)

[87] The fact that the paranoid target of a search has no expectation of privacy cannot negative his s. 8 rights: see Tessling, at para. 42. Nor can ubiquitous state intrusions upon privacy render expectations of privacy unreasonable for the purposes of s. 8: see Patrick, at para. 14. The ultimate question is whether the personal privacy claim advanced in a particular case must, upon a review of the totality of the circumstances, be [page346] recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society: see James A.Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core of Section 8?" (2005), 23 C.R. (6th) 245.

[88] As has repeatedly been said, the reasonable expectation of privacy inquiry is contextual and looks at the totality of the circumstances: Edwards, at paras. 31-45; Tessling, at paras. 19 and 31; and Patrick, at para. 26. Importantly, this contextual examination has no regard to the product of the challenged search or seizure. The inquiry is framed in "broad and neutral terms": Wong, at p. 50 S.C.R.; see, also, Buhay, at para. 19; Patrick, at para. 32. The question is not whether the appellant had a reasonable expectation that he could access and possess child pornography anonymously. The question is whether the appellant had a reasonable expectation that he could anonymously access the Internet on his computer without the state, with the co-operation of the appellant's ISP, being able to find out what he had accessed.

(iii) The application of the principles to this case

[89] The appellant presents his privacy claim as informational in nature. He asserts a right to privacy as against the state in certain information held by a third party, Bell Sympatico. The appellant maintains that the right to privacy over that information arises because if the information is disclosed to the state, the state will be able to identify some of the appellant's Internet activity and thereby obtain personal information that could reveal intimate details about the appellant's lifestyle and personal choices: see Plant, at

p. 293 S.C.R. Given that the information provided to the police by Bell Sympatico ultimately revealed the appellant as the person who accessed child pornography on three occasions, it is difficult to argue with the contention that the information provided by Bell Sympatico had the potential to open doors into very private aspects of the appellant's lifestyle.

[90] I agree with the parties that the issue is properly framed in terms of a claim to privacy in information. In so holding, I do not ignore the fact that the activity was carried out in the appellant's residence, thereby potentially raising a territorial privacy claim of the highest order. However, the physical location where the Internet activity occurred seems entirely incidental to the activity itself. The appellant's privacy claim comes down to an assertion of a reasonable expectation of anonymity when on the Internet. The anonymity claim is tied to the nature of the [page347] activity, not to the location where the activity occurs. For that reason, this case is distinguishable from cases like Tessling and Gomboc, in which the activities potentially revealed to the police had a strong physical connection to the claimant's residence.

[91] Not only is the appellant's privacy claim advanced in relation to information, that information was obtained from a third party, Bell Sympatico, who had acquired it from the appellant in the course of a commercial relationship. The Supreme Court of Canada has addressed this kind of privacy claim in Plant, Tessling and Gomboc. Those cases identify a number of factors relevant to the reasonable expectation of privacy inquiry. I propose to examine the factors that are important in the circumstances of this case by addressing three questions:

-- What was the subject matter of the impugned state conduct, that is, what were the police after when they asked Bell Sympatico for the subscriber information?

-- Did the appellant have a subjective expectation that he could act with anonymity, at least with regard to the state, in his Internet activity?

-- If so, was that expectation objectively reasonable?

(a) The target of the police action

[92] As discussed earlier, the police were after information that would potentially identify the appellant, not merely as a Bell Sympatico subscriber, but a person who had engaged in certain activities on three specific occasions on the Internet. The information sought by the police would strip the appellant of his Internet anonymity on those three occasions. This characterization of the target of the police action is not in any way altered because the information provided by Bell Sympatico would not conclusively identify the appellant as the person engaged in those activities. The information would connect his account to those activities and go some distance to identifying him as the person involved in those activities.

[93] Information that has the very real potential to reveal activities of a personal and private nature is, in my opinion, "information which tends to reveal intimate details of the lifestyle and personal choices of the individual": Plant, at p. 293 S.C.R. It follows that information that has the potential to reveal activities of that kind may be deserving of constitutional protection. The nature of the information does not, however, mean that it automatically attracts constitutional protection under s. 8. The totality of the circumstances must be considered. [page348] Where the information has been given by the claimant to a third party who in turn provides it to the police, the relationship between the claimant and that third party as it relates to the information is of critical importance. I will turn to that relationship after addressing the appellant's subjective expectation of privacy.

(b) The subjective expectation of privacy

[94] The trial judge found that the appellant had a subjective expectation of privacy in respect of his subscriber information. When, as in my view it should be, the information is characterized as information revealing the appellant's Internet activity, there can be no doubt that he had a subjective expectation of privacy. The appellant did not reveal his identity when accessing the sites and used temporary

anonymous e-mail addresses suggesting a clear intention to conceal his identity even further. The Crown's submission that the appellant was not "fussed about keeping his name and address private" misses the distinction between identifying the appellant as a Bell Sympatico subscriber and identifying the appellant's Internet activity. I think the appellant was clearly "fussed" about keeping his identity private as it related to his Internet activities.

(c) Is the expectation objectively reasonable: The relationship between the appellant and Bell Sympatico

[95] The appellant and Bell Sympatico had a commercial relationship whereby Bell Sympatico provided a variety of services, including Internet access to the appellant for a fee. Unlike for example a doctor-patient relationship, there was nothing inherently confidential in the relationship between Bell Sympatico and the appellant. In the private law context, their relationship, including any obligation Bell Sympatico had to maintain the confidentiality of information provided by the appellant, was governed by the terms of the service agreement between Bell Sympatico and the appellant, related documents referred to in the service agreement and the terms of PIPEDA. As Gomboc demonstrates, it is necessary to look at the controlling contractual and legislative provisions when determining whether a person has a reasonable expectation of privacy in information that a third party service provider has given to the police.

[96] To properly describe the relationship between the appellant and Bell Sympatico, one must first properly characterize Bell Sympatico's relationship with the police insofar as the request for the appellant's subscriber information is concerned. [page349] On this record, Bell Sympatico was not an agent of the police. Bell Sympatico had information in its possession over which it clearly had an interest. Bell Sympatico was not compelled by any statute to provide the information to the police. It chose to do so when faced with a very specific and narrow request and when made aware of the nature of the investigation: see Gomboc, at para. 42, Deschamps J., concurring; [See Note 3 below] see, also,

McNeice, at paras. 41-45.

[97] Like any service provider, Bell Sympatico had a legitimate interest in preventing the criminal misuse of its services, particularly in circumstances where the misuse effectively constituted the actus reus of a crime. That interest may be seen as purely a self-interest or, perhaps more appropriately, as a form of "civic engagement" reflecting a corporate commitment to assist in law enforcement's struggle to rid the Internet of child pornography: see Gomboc, at paras. 41-42, Deschamps J., concurring; Slane and Austin, at p. 490.

[98] The normative nature of the reasonable expectation of privacy analysis and the value judgments that underlie that analysis require that Bell Sympatico's legitimate interests, whether described as self-interest, civic engagement or both, be taken into account in determining whether the appellant had a reasonable expectation of privacy in respect of the information held by Bell Sympatico. A reasonable and informed person considering whether society would find it reasonable for the appellant to have a reasonable expectation of privacy in his subscriber information would take into account Bell Sympatico's legitimate interests in voluntarily disclosing that information to the police when that disclosure would assist in an investigation of the alleged criminal misuse of Bell Sympatico's services, assuming the disclosure was not prohibited and would not violate any laws or the terms of applicable customer agreement.

[99] Bell Sympatico's legitimate interest in disclosing customer information to the police finds expression in the terms of PIPEDA. Those terms contemplate "reasonable disclosure" of customers' personal information and recognize a discretion to disclose personal information to the police in the course of an [page350] investigation if the prerequisites of the disclosure provision are met: PIPEDA, ss. 3, 5(3) and 7(3)(c.1)(ii).

[100] Setting aside the contractual terms for the moment, I think the "reasonable and informed person" identified by Binnie J. in Patrick, at para. 14, would view a customer's reasonable

expectation of privacy in his or her subscriber information to be circumscribed by the service provider's discretion to disclose that information to the police where it was both reasonable to do so and a PIPEDA compliant request for disclosure had been made by the police.

[101] The requests made in this case complied with s. 7(3)(c.1)(ii) of PIPEDA. In considering whether Bell Sympatico acted reasonably in disclosing the information, the nature of the information sought is relevant. The police request was specific and narrow. They sought only the client's name and address. That information in and of itself revealed nothing personal about the appellant or his Internet usage. The request was also narrow in the sense that it identified three specific instances of Internet activity. By disclosing the subscriber information to the police, Bell Sympatico would not be telling the police anything about the client's Internet activities at any time other than three times identified in the requests.

[102] I think it is also significant that the request referred specifically to the investigation of child exploitation offences under the Criminal Code. Bell Sympatico was entitled to have regard to the nature of the offences being investigated when it decided whether to disclose the information. These offences are obviously serious. They victimize children, a very vulnerable element of the community and one which the community, as a whole, has a responsibility to protect. Further, Bell Sympatico's service was an integral and essential component of the offences being investigated. In a very real sense, the power and anonymity of the Internet allows these kinds of offences to be committed. The alleged perpetrator had gained access to this powerful and anonymous tool through the services provided by Bell Sympatico. The strong and direct connection between Bell Sympatico's services and the commission of the crimes under investigation would, in my view, make it all the more reasonable to expect that Bell Sympatico would co-operate with the police request for subscriber information.

[103] In stressing the nature of the offence under investigation, I do not fall into the trap of judging the

appellant's privacy expectation by reference to the nature of his activity. The nature of the offence under investigation is relevant to the reasonableness of Bell Sympatico's response to the police request. The [page351] nature of the activity that would actually be revealed to the police by the information provided by Bell Sympatico is not germane to the reasonable expectation of privacy inquiry.

[104] I see some analogy between my reliance on PIPEDA and the reliance of Abella J. in her concurring reasons in Gomboc on the terms of a regulation that allowed the utility supplier to provide information to the police absent an express request for confidentiality by the client. As Abella J. did in Gomboc, I look to legislation, the constitutionality of which is not challenged, and which by its terms speaks to the circumstances in which the third party holder of the information may disclose that information to the police as informing the degree of privacy that persons ought reasonably to expect in our society.

[105] My analysis of the impact of PIPEDA on the reasonable expectation of privacy inquiry is somewhat at odds with that of Cameron J.A., who considered the provincial equivalent to PIPEDA in Trapp, at paras. 49-54. I agree with Cameron J.A. that the reasonable expectation of privacy inquiry must proceed on the basis that the service provider will exercise "a meaningful measure of independent and informed judgment" in deciding whether to make the disclosure requested by the police: at para. 55. However, I am satisfied that having regard to the nature of the disclosure requested in this case, and the nature of the crimes being investigated, that the reasonable informed person would accept that it was reasonable for the ISP to make the disclosure requested. If disclosure by the ISP was a reasonable response to the request, then, in these circumstances, the appellant's privacy claim in the face of the request is not objectively reasonable.

[106] I come finally to the contractual terms. Unlike the provision in Gomboc, there is no legislative authority underlying the terms of the service agreement between Bell Sympatico and the appellant. Also, the caution sounded by Deschamps J. in Gomboc, at para. 33, against reliance on the

terms of contracts of adhesion when deciding constitutional rights has application here.

[107] The contractual provisions in this case tend to reinforce my reliance on PIPEDA as indicative of the nature of the appellant's reasonable expectation of privacy. Like PIPEDA, the contractual terms speak both of Bell Sympatico's duty to protect the privacy of clients' information and its willingness to disclose information in relation to investigations involving the alleged criminal misuse of its services. That willingness clearly qualifies any duty of confidentiality assumed by Bell Sympatico. While there is no single provision in the agreement or related documents that spells out Bell Sympatico's willingness to disclose [page352] information to the police as clearly as did the regulation under consideration in Gomboc, the overall thrust of the documentation is to the same effect. In particular, the accepted use policy ("AUP") makes it clear that uploading or downloading child pornography is a breach of the AUP and that Bell Sympatico would "offer full cooperation with law enforcement agencies in connection with any investigation arising from a breach of this AUP". That co-operation would, it seems to me, obviously extend to the disclosure of subscriber information which, by the terms of the service agreement, could be disclosed if "[n]ecessary to satisfy any laws, regulations or other governmental request . . . or as necessary . . . to protect . . . others".

[108] My review of the terms of the service agreement and related documents reinforces my view that a reasonable and informed person would not expect that society should recognize that the appellant had a reasonable expectation of privacy in respect of the subscriber information held by Bell Sympatico.

[109] I stress that the conclusion in this case is based on the specific circumstances revealed by this record and is not intended to suggest that disclosure of customer information by an ISP can never infringe the customer's reasonable expectation of privacy. If, for example, the ISP disclosed more detailed information, or made the disclosure in relation to an investigation of an offence in which the service was not directly implicated, the reasonable expectation of privacy

analysis might yield a different result. Similarly, if there was evidence that the police, armed with the subscriber's name and address, could actually form a detailed picture of the subscriber's Internet usage, a court might well find that the subscriber had a reasonable expectation of privacy. Those cases will be considered using the totality of the circumstances analysis when and if they arise.

Issue #2: The Adequacy of the ITO

[110] The appellant's second ground of appeal challenges the information to obtain the search warrant (ITO) that authorized the search of the appellant's residence and computer. Counsel argues that even if all of the material contained in the ITO was properly included in that document, it did not provide sufficient grounds upon which the warrant could be issued. Counsel places heavy reliance on R. v. Morelli, [2010] 1 S.C.R. 253, [2010] S.C.J. No. 8, 2010 SCC 8. In Morelli, the court found that a warrant authorizing the search of an individual's computer for child pornography ought not to have been issued as it did not provide grounds upon which a justice of the peace could reasonably [page353] believe that the named person possessed child pornography on his computer.

[111] The appellant made a similar argument at trial but did not have the benefit of Morelli. The trial judge found that the ITO contained sufficient grounds upon which the justice of the peace acting judicially could issue the warrant. He concluded that many of the appellant's arguments demonstrated only that the grounds in the ITO did not establish that the appellant had committed the offences referred to in the ITO. The trial judge correctly pointed out that the ITO need only provide reasonable grounds to believe that evidence relating to the offences would be found in the searches. The appellant's ultimate culpability was irrelevant to whether the warrant should issue.

[112] The standard of review applicable to this argument is well settled. The trial judge was obliged to determine whether there were grounds upon which the issuing justice could grant the warrant. This court applies the same deferential standard: R. v. Garofoli, [1990] 2 S.C.R. 1421, [1990] S.C.J. No. 115, at p. 1452 S.C.R. Morelli is an example of the application of the

well-established Garofoli standard of review to the particular facts of that case. Morelli breaks no new jurisprudential ground.

[113] This ITO is very different from the ITO found to be deficient in Morelli. Most significantly, this ITO provided strong evidence from which it could be inferred that someone using the appellant's computer at his residence had accessed or downloaded child pornography on eight instances, six on June 16, 2006 and one each on July 2 and 6, 2006. These allegations, in my view, provided a basis upon which the justice could infer that there was a reasonable probability that child pornography had been accessed and stored on the computer. Unlike Morelli, the police in this case sought the warrant both in respect of the offence of accessing child pornography and the offence of possessing child pornography. In Morelli, the police sought a warrant only in respect of the possession charge.

[114] The ITO also provided extensive technical evidence to the effect that files downloaded by the appellant on the computer could be recovered by police technicians even if the appellant had made efforts to delete those files. This evidence offered some basis for an inference that the prohibited material remained on the computer long after it was downloaded and could be recovered if the police were given access to the computer.

[115] The affiant also provided detailed evidence based on his first-hand experiences about the practices of individuals who access and possess child pornography on their computers. He indicated that often these individuals kept images for "long [page354] periods of time" and "rarely deleted collections". I see no reason why this kind of evidence, rooted in the officer's personal experience, could not provide some assistance in determining whether the warrant should be granted. I bear in mind that the officer's opinion did not stand alone. There was other reliable evidence that this computer had been used to access child pornography on three occasions over a three-week period, suggesting use of the computer by someone with an interest in child pornography.

[116] The technical evidence and the officer's opinion evidence provided a basis upon which a justice of the peace could reasonably infer that there was a reasonable probability that the child pornography that had been accessed on the computer some ten months earlier was still on the computer and could be retrieved by the police. That is all that was needed to justify the issuance of the warrant. This ground of appeal fails.

IV

Conclusion

[117] I would dismiss the appeal.

Appeal dismissed.

Notes

Note 1: In Tessling, at para. 40, Binnie J. states "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public". In my view, this comment is not directed at cases where the person acts anonymously: see, also, Wise, at p. 558 S.C.R., La Forest J., dissenting.

Note 2: The "risk analysis" favoured in the American case law would doom the appellant's argument since the subscriber information was willingly disclosed to the appellant's ISP: e.g., see United States of America v. Perrine, 518 F. 3d 1196 (10th Cir. 1998), at pp. 1204-1205 F. 3d; United States of America v. Bynum, 604 F. 3d 161 (4th Cir. 2010), at p. 164 F. 3d. Recently, in United States v. Jones, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012), Sotomayor J., in a concurring opinion, suggested [at p. 957 S. Ct.] that the risk analysis approach was "ill suited to the digital age in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks". She opined that it may be time to reconsider the court's approach to privacy claims under the Fourth Amendment.

Note 3: The dissent in Gomboc views the utility company as

having been conscripted to assist the police. This conclusion seems to be based on the utility company's installation, at the request of the police, of a special device used to generate, record and disclose the relevant information. Here, Bell Sympatico did nothing other than provide information from its database.
