C-50206

COURT OF APPEAL FOR ONTARIO

B E T W E E N

HER MAJESTY THE QUEEN

Respondent

– and –

DAVID WARD

Appellant

APPELLANT'S FACTUM

MICHAL FAIRBURN
MINISTRY OF THE ATTORNEY GENERAL FOR ONTARIO
Crown Law Office – Criminal
720 Bay Street, 10th Floor
Toronto, Ontario
M5G 2K1

Tel: 416-326-2002
Fax: 416-326-4656
email: michal.fairburn@ontario.ca

COUNSEL FOR THE RESPONDENT

JONATHAN DAWE
SACK GOLDBLATT MITCHELL LLP
20 Dundas Street West
Suite #1100
Toronto, Ontario
M5G 2G8

Tel: 416-979-6447
Fax: 416-591-7333
email: jdawe@sgmlaw.com

COUNSEL FOR THE APPELLANT

C50206

COURT OF APPEAL FOR ONTARIO

B E T W E E N

HER MAJESTY THE QUEEN

Respondent

– and –

DAVID WARD

Appellant

APPELLANT'S FACTUM

TABLE OF CONTENTS

PART I: STATEMENT OF THE CASE

1. In May, 2007 the Appellant was charged with a single count each of possessing[1] and accessing[2] child pornography. The Crown proceeded by indictment and the Appellant elected to be tried in the Ontario Court of Justice. His trial was held in Sudbury before the Hon. Mr. Justice Lalande. In June, 2008 the Appellant brought a pre-trial *Charter* motion asserting breaches of his s. 8 *Charter* rights. On August 8, 2008 the trial judge found no breaches and dismissed the application. The trial then proceeded on the basis of an uncontested statement of facts, and the Appellant was convicted as charged. On December 16, 2008, he was sentenced to 11 months imprisonment. The Appellant filed an Inmate Notice of Appeal against both conviction and sentence. In March, 2009 he filed a Solicitor's Notice of Appeal against conviction only and abandoned his sentence appeal. He has fully served his custodial sentence.

> Information of D. Beck, sworn May 25, 2007, *Appeal Book*, pp. 9-13
> Ruling on *Charter* Motion, dated August 8, 2008, *Appeal Book*, pp. 14-37
> Solicitor's Notice of Appeal, filed March 20, 2009, *Appeal Book*, pp. 1-4
> Notice of Abandonment of Sentence Appeal, filed March 30, 2009, *Appeal Book*, pp. 5-8

2. The main issue in this appeal is whether the police should require a search warrant in order to obtain information from Internet service providers about their subscribers' Internet activities – specifically, the Internet Protocol addresses ("IP addresses") assigned to a particular subscriber (or, equally, the identity of the subscriber assigned a particular IP address). This is an issue of considerable general public importance which has divided the lower courts.[3]

> *R. v. Cuttell* (2009), 247 C.C.C. (3d) 424 (Ont. C.J.)

---

[1] *Criminal Code*, s. 163.1(4)
[2] *Criminal Code*, s. 163.1(4.1)
[3] In the case at bar, the trial judge found that ISP subscribers have no reasonable expectation of privacy over this information. In a later decision, *R. v. Cuttell, infra*, the trial court reached the opposite conclusion. *Cuttell* is also under appeal to this Court, and all counsel have agreed to take steps to have the two appeals heard together. The Canadian Civil Liberties Association has indicated it will be seeking leave to intervene.

PART II: SUMMARY OF THE FACTS

A. The Internet and Internet Protocol Addresses ("IP Addresses")

3. The Internet allows data and information to be transferred between computers around the world. Most users gain access to the Internet through a commercial Internet Service Provider ("ISP"). There are a number of Canadian ISPs, including Bell Sympatico. To use the Internet, a computer must be assigned an Internet Protocol address ("IP address").[4] Every ISP has a collection of unique IP addresses which it reassigns to its subscribers. Subscriber IP address assignments are usually temporary, and over time subscribers typically have multiple different IP addresses assigned to their accounts. Bell Sympatico keeps records of the dates and times that a particular IP address is assigned to a particular subscriber.

> Information to Obtain Search Warrant of Det. Cst. Timothy Burtt, sworn May 22, 2007 [hereinafter "ITO"] at ¶130, 133-134, Affidavit of A. Furgiuele, sworn April 3, 2008, Exhibit C *Appeal Book*, Tab 2C, pp. 41-42
> Affidavit of Russ Doucet, sworn May 7, 2008, ¶2-4, *Appeal Book*, Tab 3, pp. 2-3

4. A computer that connects to the Internet through a direct connection with an ISP's network will be assigned a unique IP address. However, computers can also be connected to an ISP through a wired or wireless local area network. A wireless network links multiple computers by radio to a central device known as a wireless access point (WAP), which is connected to the ISP's network. The ISP assigns a unique IP address to the WAP. All computers connecting to the Internet through the wireless network then share this IP address. Bell Sympatico keeps records of its IP address assignments to subscribers, but not of the specific computers using these addresses. If a wireless network is unsecured, anyone within the network's range (typically about 300 feet) can connect to the Internet using the IP address assigned to the WAP, without the subscriber's knowledge and/or permission.

---

[4] An IP address is a unique number, usually represented as a series of four 1- to 3- digit numbers separated by decimal places (e.g., 69.159.10.48).

ITO, ¶133-34, *Appeal Book*, Tab 2C, p. 42
Affidavit of Russ Doucet, sworn May 7, 2008, ¶22-28, *Appeal Book*, Tab 3, pp. 15-18

B. The German Police Investigation

5. On July 7, 2006 the owner of a German website[5] informed the authorities that 28 of the site's approximately 25,000 forums had been used to post child pornography. These forums were publicly accessible to anyone with an Internet connection who had registered and provided an e-mail address. Whenever a forum was accessed, the website's software would record the date and time, the associated IP address, and the e-mail address the user had provided. The German police determined that objectionable content was accessed – *i.e.*, uploaded or downloaded – on 229 occasions by computers using IP addresses registered to Canadian ISPs. In August or September, 2006,[6] INTERPOL sent the RCMP a list of these IP addresses and the dates and times they had accessed objectionable content.

ITO at ¶31-33, 36, 42-53 *Appeal Book*, Tab 2C, pp. 21-26
Interpol Wiesbaden Dispatches, dated August 23, 2006 and November 30, 2006, p. 2, Affidavit of A. Furgiuele, Exhibit E, *Appeal Book*, Tab 2E, pp. 61-67

C. The RCMP's *PIPEDA* Request

6. The RCMP determined that three of the IP addresses on this list were associated with Bell Sympatico in Sudbury:

IP Address	Accessing Date	Time (GMT)	Duration
69.159.6.125	16 June 2006	06:09:24 - 06:09:48	24 seconds
69.159.10.48	2 July 2006	04:35:40	1 second
69.159.7.45	6 July 2006	06:06:04	1 second

On all three occasions the person accessing the website had used a temporary disposable e-mail address. On November 22, 2006 the RCMP sent three "letters of request" to Bell Canada's Montreal offices seeking to identify subscribers assigned these IP addresses on these occasions. The letters stated that this information was being requested "in accordance with s. 7(3)(*c*.1) of

[5] <www.carookee.com>
[6] Det. Cst. Burtt's ITO initially states that this information was provided to the RCMP on August 23, 2006 (at ¶50), but later states that the RCMP only received it on September 20, 2006 (at ¶52).

the *Personal Information Protection [and] Electronic Documents Act*", and explained that the RCMP was **"**conducting an investigation in relation to child sexual exploitation offences under the *Criminal Code*". The letters did not reveal any further detail about the particular nature of the investigation or the relevance of the information sought. Bell Sympatico responded by identifying the Appellant as the subscriber on all three specified occasions and providing his home address.

ITO at ¶24, 45, 50, 53-58, *Appeal Book*, Tab 2C, pp. 19, 24-27
Letters of Request for Account Information Pursuant to a Child Sexual Exploitation Investigation from Cst. J. Tree to Bell Canada, dated November 22, 2006 (×6), Affidavit of A. Furgiuele, Exhibit D, *Appeal Book*, Tab 2D, pp. 55-60
Interpol Wiesbaden Dispatches, dated August 23, 2006 and November 30, 2006, Affidavit of A. Furgiuele, Exhibit E, *Appeal Book*, Tab 2E, pp. 61-67
Personal Information Protection and Electronic Documents Act ("PIPEDA"), S.C. 2000, c. 5, s. 7

D. The Sudbury Police Investigation

7. On December 6, 2006 the RCMP advised the Sudbury Regional Police of the results of its *PIPEDA* request. On January 2, 2007 they forwarded a database summarizing the details of the three accessing incidents in June and July, 2006. DC Timothy Burtt viewed the accessed images and concluded they fell within the Canadian legal definition of child pornography.[7]

ITO at ¶72-90, *Appeal Book*, Tab 2C, pp. 29-31

E. Technical Background Evidence re Internet Browser File Downloads

8. The Appellant tendered an affidavit from a computer expert addressing various technical matters. Among other things, the affidavit explained how image files on web pages can be downloaded to a computer hard drive without the user's knowledge, and sometimes without the image ever being visible on the user's screen. The Crown declined to cross-examine the defence expert and his evidence on these points was uncontroverted.

Affidavit of Russ Doucet, ¶1-21, *Appeal Book*, Tab 3, pp. 2-14

[7] During the 24-second visit on June 16, 2006, six different images were accessed. During the two one-second visits on July 2 and 6, 2006 a single image was accessed (the same image both times). The images all depicted prepubescent boys with erect penises.

R. v. Garbett, 2008 ONCJ 97 at ¶22-24, 51-52, *aff'd* 2010 ONSC 2762
R. v. Morelli, 2010 SCC 8, 282 C.C.C. (3d) 273 at ¶34-37

F. The Sudbury Police Investigation

9. After receiving the Appellant's name from the RCMP, DC Burtt made some preliminary inquiries that confirmed the Appellant's address but revealed nothing further of consequence.[8] Three times between December, 2006 and April, 2007 he drove past the Appellant's home. On April 22, 2007, a different Sudbury officer went to the Appellant's home, knocked on the door and advised the Appellant (untruthfully) that he was investigating an e-mail harassment complaint. The Appellant told the officer that he lived alone and that he had a computer with Internet access "but it was not wireless".[9] The Sudbury police took no other steps to investigate the Appellant before obtaining a warrant to search his home.

ITO, ¶18-19, 59-71, 91-109, 117-24 *Appeal Book*, Tab 2C, pp. 18, 27-28, 32-35, 39-40

G. The Search of the Appellant's Home

10. On May 22, 2007 DC Burtt applied for a s. 487 *Criminal Code* warrant to search the Appellant's home and seize, *inter alia*, computers and data storage devices. His Information to obtain this warrant ("the ITO") contained a section titled "Child Pornography Collections" that set out generalizations about the propensity of child pornography collectors to hoard images in their homes. However, no individualized grounds were presented to indicate that the Appellant himself had such a collection in his home. The only evidence specifically relating to the Appellant was the evidence that his Sympatico account had been used on three occasions in June

[8] Specifically, DC Burtt conducted driver's licence record and telephone directory searches which confirmed the Appellant's address, a Google Internet search that revealed that he worked at the local YMCA, and searches of Sudbury police records that revealed that he had no criminal record or police history.
[9] It is unclear what the Appellant told the police about his ISP subscription. At ¶99 of his ITO DC Burtt states that the Appellant told the officer he was a Bell Sympatico subscriber, but at ¶124 of the same document he maintains that the Appellant identified his ISP as "Persona Inc/Communications".

and July, 2006, for a total of 26 seconds, to access web pages containing child pornographic images.

ITO, ¶155-65, *Appeal Book*, Tab 2C, pp. 49-50

11. The search warrant was issued on May 23, 2007 and executed the following day. The Appellant was home alone. After entering the house the police observed a computer screen displaying child pornographic images. The Appellant was arrested and charged with one count each of possessing and accessing child pornography.[10] The police seized four computers, a wireless router and various documents and data storage media. Subsequent forensic analysis of the computer hard drives revealed numerous child pornographic images, along with an extensive quantity of lawful adult pornography.

Search Warrant, issued May 23, 2007, Affidavit of A. Furgiuele, Exhibit B, *Appeal Book*, Tab 2B, pp. 8-10
Report to a Justice, signed June 13, 2007, Affidavit of Andrew Furgiuele, Exhibit F, *Appeal Book*, Tab 2F, pp. 68-83
Image Reports (Exhibits 1-3B); *Appeal Book*, pp. 28-72
Information of D. Beck, sworn May 25, 2007, *Appeal Book*, pp. 9-13

H. The Appellant's Trial

12. The Appellant brought a pre-trial *Charter* application alleging two distinct breaches of his s. 8 *Charter* rights. First, he argued that his s. 8 rights were infringed when the police obtained information about his IP address allocation history from Bell Sympatico without judicial authorization. Second, he argued that the search warrant for his home was unsupported by reasonable grounds to believe that evidence of an offence would be found in his residence. As a remedy, he sought to have the seized evidence excluded under s. 24(2) of the *Charter*. The trial judge found no s. 8 *Charter* breaches and did not address the issue of s. 24(2) exclusion.

Notice of Application dated April 2, 2007, *Appeal Book*, Tab 1, pp. 1-4
Ruling on *Charter* Motion, *Appeal Book*, pp. 14-37

[10] The possession count was particularized as occurring on May 24, 2007 (the date of the search), while the accessing count was particularized as occurring between June 16 and July 6, 2006 (the first and last of the three dates when the Appellant's ISP account accessed the German web site).

PART III: ISSUES AND THE LAW

13. The central question in this appeal is whether the *Charter* requires the police to obtain prior judicial authorization before seeking information from Internet service providers about subscribers' IP address allocation histories – information that can reveal details of subscribers' Internet activities. This issue has significant implications for Canadians' right to privacy on the Internet, and raises important policy questions about whether state intrusions on this privacy should be judicially regulated. The lower courts in Ontario and elsewhere have divided on this point. Some courts have found that ISP subscribers have a reasonable expectation of privacy over their IP address histories that this information is thus protected by s. 8 of the *Charter* and ordinarily only accessible to the police with a warrant.[11] Other courts have reached the opposite result, relying on various different rationales to conclude that no reasonable expectation of privacy should be recognized over this information, removing it from the ambit of s. 8 and making it freely available to the police on request.[12] No Canadian appellate court has yet ruled on this issue.[13]

14. The second issue in this appeal concerns the adequacy of the grounds supporting the search of the Appellant's home. Even assuming, *arguendo,* that the police lawfully obtained the Appellant's IP address history, it is submitted that they lacked reasonable grounds to believe that the he had committed the offence of possession of child pornography (as distinct from accessing). More importantly, they lacked reasonable grounds to believe that evidence of either offence would be found in his home on the date of the search, almost eleven months after the last

---

[11] See *R. v. Cuttell, supra*; *R. v. Kwok*, [2008] O.J. No. 2414 (S.C.J.); *Re C.(S.),* [2006] O.J. No. 3754 (C.J.)

[12] See Ruling on *Charter* Motion, ¶25-70, *Appeal Book,* pp. 19-30; *R. v. F.(S.W.),* 2008 ONCJ 740; *R. v. Wilson,* 2009 O.J. No. 1067 (S.C.J.); *R. v. Vasic,* 2009 CanLII 6842 (Ont. S.C.J.); *R. v. McGarvie,* 2009 CarswellOnt 500 (C.J.); *R. v. Verge,* 2009 CarswellOnt 501 (C.J.); *R. v. Brousseau,* 2010 ONSC 6753; *R. v. Trapp,* 2009 SKPC 5; *R. v. McNeice,* 2010 BCSC 1544.

[13] The Saskatchewan Court of Appeal heard argument on the issue in November, 2010 in an appeal from the trial judgment *R. v. Trapp, supra*, but as of January, 2011 the Court's judgment is still on reserve.

known occasion when his ISP account had accessed suspect files. The trial judge, who upheld the validity of the warrant, did not have the advantage of the Supreme Court of Canada's recent decision in *R. v. Morelli, supra*, which bears directly on both issues. Finally, if any *Charter* breaches are found the admissibility of the seized evidence under s. 24(2) must be considered.

Ruling on *Charter* Motion, ¶71-111, *Appeal Book,* pp. 30-37
R. v. Morelli, supra

A. Issue 1: IP Address Histories and the *Charter*

1) Framing the *Charter* Issue: *PIPEDA* and Section 8

15. Section 8 of the *Charter* protects "informational privacy" – "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[14] When the police request and obtain information about a person from a third party, s. 8 will be engaged if the subject person had a "reasonable expectation of privacy" over the information.[15] The critical question in the case at bar is whether the Appellant had a reasonable expectation of privacy over information in Bell Sympatico's files concerning the assignment of specific IP addresses to his account.

16. *PIPEDA* is privacy-protecting legislation.[16] It prohibits private commercial organizations – including ISPs – from divulging "personal information" about people without their knowledge and consent.[17] This general rule is subject to various exceptions. In particular, s. 7(3)(c) authorizes disclosure as "required to comply with a subpoena or warrant" or other court order. Section 7(3)(*c*.1)(ii) goes further and permits disclosures:

---

[14] *R. v. Tessling*, 2004 S.C.C. 67, 189 C.C.C. (3d) 129 at ¶23.
[15] See, *e.g.*, *R. v. Plant* (1993), 84 C.C.C. (3d) 203 (S.C.C.); *R. v. Law* 2002 S.C.C. 10, 160 C.C.C. (3d) 449 at ¶15. In this situation it is irrelevant whether or not the third party has voluntarily cooperated with the police, since consent will give rise to a valid waiver of s. 8 rights only when "the giver of the consent had the authority to give the consent in question": *R. v. Wills* (1992), 70 C.C.C. (3d) 529 at p. 546 (Ont. C.A.). See, *e.g.*, *R. v. Dyment* (1988), 45 C.C.C. (3d) 244 (S.C.C.); *R. v. Wong* (1990), 60 C.C.C. (3d) 460 (S.C.C.); *R. v. Mercer* (1992), 70 C.C.C. (3d) 180 at pp. 184-90 (Ont. C.A.); *R. v. Buhay* (2003), 174 C.C.C. (3d) 97 (S.C.C.)
[16] See, *e.g.*, the legislation's statement of purpose in s. 3.
[17] *PIPEDA*, ss. 2, 4.

> … 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]

Although s. 7(3)(*c.*1) contemplates situations where personal information can be disclosed to the police without a court order, it contains the important restriction that the police must have "lawful authority to obtain the information". *PIPEDA* itself does not provide the police with the requisite "lawful authority". When information is protected by s. 8 of the *Charter* – that is, when the person to whom it relates has a "reasonable expectation of privacy" over it – the "lawful authority" requirement has a further constitutional dimension: police requests for protected information are searches and/or seizures that will violate s. 8 unless "authorized by law".[18]

PIPEDA, ss. 2-4, 7

17. When s. 7(3)(*c.*1) was added to *PIPEDA* late in the legislative process, it was presented to the House of Commons as merely "allow[ing] the *status quo* to continue"[19] and not "grant[ing] new powers to government institutions".[20] The trial judge in the case at bar agreed that s. 7(3)(*c.*1) "does not create a new search power or defeat a person's *Charter* protection against unreasonable search and seizure".[21] The provision's impact is thus limited. It permits organizations to cooperate with police requests by releasing information that is *unprotected* by s. 8 of the *Charter* (*i.e.*, that does not attract a "reasonable expectation of privacy"). It also permits organizations to release *s. 8 protected information* when the police can point to a specific

---

[18] See *R. v. Law*, *supra* at ¶15; *R. v. Collins* (1987), 33 C.C.C. (3d) 1 at p. 14 (S.C.C.); *Hunter v. Southam Inc.* (1984), 14 C.C.C. (3d) 97 (S.C.C.)
[19] Parliamentary Secretary to the Minister of Industry, *Hansard*, October 20, 1999, pp. 412-13.
[20] Minister of Industry, *Hansard*, October 22, 1999, pp. 538-39.
[21] See the decision on appeal at ¶57; *R. v. Cuttell*, *supra* at ¶40; *R. v. C.(S.)*, *infra* at ¶9; *R. v. Kwok*, *supra* at ¶32-35.

statutory or common law power authorizing them to seize the information without a warrant.[22] However, the police cannot use s. 7(3)(*c*.1) to obtain *Charter*-protected private information they have no legal authority to seize without a warrant. Permitting this would eviscerate the s. 8 *Charter* prior authorization regime and leave the protection of privacy up to the discretion of private businesses rather than the judiciary.

> Hansard, October 20, 1999, pp. 412-13; October 22, 1999, pp. 538-39
> Ruling on *Charter* Motion, *supra* at ¶57, *Appeal Book*, pp. 26-27
> J. Stoddart, "Customer Name and Address (CNA) Information Consultation Document: Response of the Office of the Privacy Commissioner of Canada", October, 2007, p. 4

2) Policy Considerations

a) Expectations of Privacy and Technological Change

18. Section 8 of the *Charter* and the underlying concept of "reasonable expectations of privacy" must be understood and applied purposively and contextually. As the Supreme Court of Canada has repeatedly emphasized, "[e]xpectation of privacy is a normative rather than a descriptive standard".[23] Courts that apply and interpret s. 8 are called on to determine whether Canadians should be entitled to privacy vis-à-vis the state in a particular context. In *R. v. M.(A.)*, *infra*, Binnie J., writing for the majority on this point, stated:

> Section 8, like the rest of the *Charter*, must be interpreted purposively, that is to say, to further the interests it was intended to protect. … A privacy interest worth of protection is one the citizen subjectively believes ought to be respected by government and "that society is prepared to recognize as 'reasonable'".[24]

The legal backdrop created by legislation and private contracts is a relevant factor to consider but cannot be dispositive. The *Charter* ultimately constrains legislation, not the other way

---

[22] For example, s. 487.11 of the *Criminal Code* authorizes warrantless searches and seizures when the police have grounds to obtain a warrant but are faced with "exigent circumstances" that make it "impracticable" to do so. In this situation, s. 7(3)(*c*.1) would permit a third party to disclose s. 8-protected information to the police without the subject's consent. Exigent circumstances can also sometimes trigger other disclosure provisions of *PIPEDA* (see, *e.g.*, *PIPEDA* s. 7(*e*), which authorizes the disclosure of information "because of an emergency that threatens the life, health or security of an individual").

[23] *R. v. Tessling*, *supra* at ¶42; *R. v. M.(A.)* (2008), 230 C.C.C. (3d) 377 at ¶65 *per* Binnie J. (S.C.C.); *R. v. Patrick*, 2009 SCC 1, 242 C.C.C. (3d) 158 at ¶12; *R. v. Gomboc,* 2010 S.C.C. 55 at ¶34, *per* Deschamps J., at ¶115, *per* McLachlin C.J.C. and Fish J., (dissenting in the result).

[24] *R. v. M.(A.), supra* at ¶33, quoting from the United States Supreme Court decision in *United States v. Katz*, 389 U.S. 347 (1967). See also *R. v. Wong*, *supra* at p. 478; *R. v. Patrick*, *supra* at ¶14.

around, and laws authorizing state intrusions on privacy cannot be shielded from s. 8 *Charter* scrutiny by the argument that their very existence snuffs out all expectations of privacy. Likewise, the normative and profoundly important social question of how much privacy citizens should expect cannot be dictated by contractual terms drafted by private businesses.

19. In *R. v. Wong*, *supra*, La Forest J. noted that "the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development."[25] Technological change affects privacy in two distinct ways. New technologies give the state new ways to snoop on citizens. They also change social habits and practices. As a new technology becomes intertwined into the fabric of Canadian life, the courts and legislatures share responsibility for ensuring that the privacy necessary in a free and open society is not unduly eroded.[26]

20. Computers and the Internet have become ubiquitous features of modern life and the repository of vast quantities of highly private information. As Fish J. recently observed in *R. v. Morelli*, *supra* (at ¶2-3):

> It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.
>
> First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have

---

[25] *R. v. Wong*, *supra* at p. 477; see also *R. v. Tessling*, *supra* at ¶55.

[26] The evolution of the law regulating the interception of mobile telephone communications provides a good illustration. When the mobile telephone was still a novelty, a few early cases held that there was no reasonable expectation of privacy in mobile phone conversations (see, *e.g.*, *R. v. Lubovac* (1989) 52 C.C.C. (3d) 551 (Alta. C.A.); *R. v. Solomon* (1992), 77 C.C.C. (3d) 264 (Que. Mun. Ct.)). However, as Canadians' use of mobile telephones dramatically increased these cases were overtaken by later decisions and statutory amendments (see, *e.g.*, *R. v. Solomon* (1993), 85 C.C.C. (3d) 496 at pp. 509-18 (Que. Mun. Ct.); *rev'd on other grounds* (1996) 110 C.C.C. (3d) 354 (Que. C.A.), *aff'd* (1997), 118 C.C.C. (3d) 351 (S.C.C.); *Criminal Code* s. 183). The end result is that mobile telephone conversations are now well-established to be private and protected by s. 8 of the *Charter*, reflecting Parliament and the courts' determination that in a free society people should be able to have private telephone conversations no matter which underlying technology they use.

> downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident. [Emphasis added]

This "electronic roadmap" can provide a highly revealing window into a person's private life. The web pages people visit and the Internet searches they conduct often reveal intimate details about their health, finances, politics, social and sexual relationships and other intensely personal matters. The central policy issue in this appeal is whether the *Charter* should regulate police efforts to reconstruct this "electronic roadmap" through information obtained from third parties.

> *R. v. Morelli*, *supra* at ¶2-3,
> Affidavit of Russ Doucet, ¶29, *Appeal Book*, Tab 3, p. 18

21. As Justice Fish noted in *Morelli*, a record of the web sites a person visits is typically retained on the user's computer hard drive. In addition, web sites often record visitors' IP addresses. The site's host servers can be located anywhere in the world, making it difficult to regulate effectively how this information is collected and disseminated. Even so, privacy still exists on the Internet: a searcher who reconstructs the cybernetic travels of a particular IP address generally cannot, without more, link this history to a specific person. The key to making this connection lies in the ISP's records of its IP address assignments. These records thus serve as the last line of defence for privacy on the Internet. The central policy question this Court must decide is whether police access to this information should be judicially regulated under the *Charter*, rather than left to the discretion of private corporations. Like the telephone, the Internet has become an unavoidable and indispensable tool of modern life. If the police have free rein to monitor Canadians' Internet usage with no constitutional checks or judicial oversight, privacy will be severely eroded. It is no response to tell Canadians that if they want their privacy they must stop using the Internet, any more than it would have been an answer in the past to tell people to stop talking on the telephone. A purposive and normative approach to s. 8 of the *Charter* demands more.

R. v. Morelli, supra at ¶3

b) Implications for Privacy of Allowing Unregulated Police Access to IP Address Histories

22. The cases to date considering warrantless police requests for IP address allocation histories have involved broadly similar facts, in two respects.[27] First, all have been child pornography cases. Second, in all cases the police had specific information linking a particular IP address to the *actus reus* of an offence and probably could have obtained a warrant to seize the associated IP address history from the ISP. However, if IP address allocation histories are held not to be private and are left entirely unprotected by the *Charter* and unregulated by the judiciary, the implications would extend much further. The police would be able to seek IP address histories in connection with *any* type of investigation, regardless of whether they had any grounds to believe a crime had actually been committed. For example, they could request subscribers' IP address history in order to examine their Internet browsing patterns for evidence of possible wrongdoing or merely to create an "intelligence" file detailing the targets' private interests and associations. They could also request the subscriber information of visitors to an entirely lawful web site, either based on some speculative association between the subject-matter of the site and criminality (e.g., a discussion board about peaceful political protests) or purely for "intelligence" purposes. If the *Charter* does not apply to IP address histories, requests for this information would be unregulated before the fact, and in most cases remain invisible after the fact. Compliance would be left to the discretion of the ISP, which would often not know why the police wanted the information.[28] The resulting erosion of personal privacy and potential for abuse would be considerable.

[27] See the cases cited at ¶13, *supra*.

[28] For instance, the *PIPEDA* requests in the case at bar simply state in very general terms the nature of the offence under investigation (see *Appeal Book*, Tab 2D). An ISP receiving such a request has no way of knowing whether the

3) Should a "Reasonable Expectation of Privacy" be Recognized Over IP Address Histories?

a) The Governing Legal Framework

23. The existence or absence of a "reasonable expectation of privacy" must be "determined on the basis of the totality of the circumstances",[29] with the particular factors considered "tailored to the circumstances of the [particular] case".[30] Potentially relevant factors include:

> … the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.[31]

When assessing whether a person has a reasonable expectation of privacy over information in the possession of a third party, the analysis will tend to focus on whether this information bears on:

> ... a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[32]

However, the Supreme Court of Canada has also cautioned that "[n]ot all information that fails to meet the 'biographical core of personal information" test is thereby open to the police."[33]

24. This analytic framework has been applied to a variety of different types of information. For example, it has been held that people have no reasonable expectation of privacy over utility records of their total electricity consumption over a six-month period,[34] over "general

---

police have specific evidence that a subscriber has committed a crime, or whether they are merely pursuing a hunch or gathering "intelligence".

[29] *R. v. Edwards* (1996), 104 C.C.C. (3d) 136 at ¶31 (S.C.C.)

[30] *R. v. Tessling*, *supra* at ¶31.

[31] *R. v. Plant, supra* at p. 212. However, the relevance of the seriousness of the offence to the threshold issue of whether a particular class of information should be characterized as private has been questioned: see, *e.g.*, Lamer C.J.C.'s concurring reasons in *Schreiber v. Canada (Attorney General)* (1998), 124 C.C.C. (3d) 129 at ¶21 (S.C.C.).

[32] *R. v. Plant, supra* at p. 213.

[33] *R. v. M.(A.), supra* at ¶68.

[34] *R. v. Plant, supra*.

information" about their banking activities,[35] over tax slips they have submitted in support of a welfare application,[36] or over expense claims they have submitted to their employer.[37] On the other hand, *Charter*-protected privacy interests have been found to exist over medical and counselling information,[38] detailed financial records,[39] and personal e-mails stored on an ISP's servers.[40] The case law on cell phone records is divided, but recent decisions have recognized an expectation of privacy over detailed records that reveal specific information about calls.[41]

25. Recently, in *R. v. Gomboc, supra* the Supreme Court of Canada considered whether a reasonable expectation of privacy should be recognized over more detailed electricity consumption records than those previously considered by the Court in *R. v. Plant, supra*.[42] The Court was sharply divided, with shifting majorities on the two major underlying legal questions:

- A five-justice[43] majority agreed that the detailed consumption data at issue was sufficiently revelatory of activities inside the home to ordinarily attract a reasonable expectation of privacy;

- A differently-constituted majority[44] held a legislatively-imposed contractual term expressly authorizing the utility to disclose this information to the police without a

---

[35] *R. v. Lillico* (1994), 92 C.C.C. (3d) 90 (Ont. Gen. Div.), *aff'd* 1999 CanLII 2836 (Ont. C.A.); *R. v. Quinn* (2006), 209 C.C.C. (3d) 278 (B.C.C.A.)
[36] *R. v. D'Amour* (2002), 166 C.C.C. (3d) 477 (Ont. C.A.)
[37] *R. v. Stymiest*, 2006 N.B.Q.B. 160
[38] *R. v. Dyment, supra*, *R. v. Mills*, (1999), 139 C.C.C. (3d) 321 at ¶77-89 (S.C.C.)
[39] *Schreiber v. Canada (Attorney General), supra*; *R. v. Chusid* (2001), 57 O.R. (3d) 20 at ¶39-46 (S.C.J.); *R. v. Eddy*, 1994 CanLII 5274 (Nfld. S.C.T.D.)
[40] *R. v. Weir* (2001), 156 C.C.C. (3d) 188 at ¶11 (Alta. C.A.)
[41] See, *e.g.*, *R. v. MacInnis*, 2007 CanLII 29342 (Ont. S.C.J.); *R. v. Mahmood* (2008), 236 C.C.C. (3d) 3 (Ont. S.C.J.) see also *R. v. Pal and Tahvili*, 2007 BCSC 1494 at ¶6-30; *R. v. Lee*, 2007 ABQB 767 at ¶283.
[42] While in *Plant*, the police had obtained data about the defendant's total household electricity consumption over 6 months, the police in *Gomboc* obtained a graph showing in detail how the defendant's usage fluctuated from minute to minute over a five-day period.
[43] Justice Abella, joined by Binnie and LeBel JJ., and the Chief Justice and Fish J., who delivered joint reasons (dissenting in the result).
[44] See the plurality reasons of Deschamps J. (Charron, Rothstein and Cromwell JJ. concurring) and the joint reasons of McLachlin C.J.C. and Fish J., dissenting in the result. Abella J. (joined by Binnie and LeBel JJ.) concurred in the result but dissented on this point, concluding that the statutorily-imposed contractual disclosure term destroyed the reasonable expectation of privacy that otherwise would have existed over the information. She noted that the constitutionality of the Alberta legislation imposing this condition had not been raised on the appeal.

> warrant was not dispositive of the privacy issue, but was merely "one factor amongst many which must be weighed in assessing the totality of circumstances".[45]

b) The Privacy Interests at Stake

26. The information obtained by the police from Bell Sympatico revealed more about the Appellant than merely his name, address and the unremarkable fact that he had home Internet service. Rather, it linked him to the use of specific IP addresses on specific past occasions, exposing his Internet browsing history and thereby opening a window into "intimate details of [his] lifestyle and personal choices".[46] Disclosing this information thus revealed considerably more about the Appellant than the disclosure of his name and address alone would have done. The central issue in this appeal is whether a reasonable expectation of privacy should be recognized over information capable of revealing details of an individual's Internet activities.

27. Canadians believe they should have a measure of privacy online. In a 2004 public opinion survey commissioned by the Public Interest Advocacy Centre, 86% of respondents agreed that the government should not be able to "monitor your Internet use without a warrant". As Seaton J.A. of the Federal Court of Appeal observed in *BMG Canada Inc. v. Doe*:[47]

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

Civil courts have also recognized the close link between Internet privacy and disclosure of users' IP address histories. In *Irwin Toy Ltd. v. Doe*[48] Wilkins J. stated:

> Implicit in the passage of information through the Internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. …

---

[45] *R. v. Gomboc, supra* at ¶31, *per* Deschamps J.; see also ¶115, *per* McLachlin C.J.C. and Fish J., dissenting in the result.
[46] *R. v. Plant, supra* at p. 213.
[47] *BMG Canada Inc. v. Doe*, 2005 FCA 193 at ¶4
[48] *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 at ¶10-11 (S.C.J.).

> Generally speaking, it is understood that a person's Internet protocol address will not be disclosed.
> …
> In keeping with the protocol or etiquette developed in the usage of the Internet, some degree of privacy or confidentiality with respect to the identity of the Internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy.
>
> Public Interest Advocacy Centre, *Consumer Privacy and State Security: Losing our Balance,* November, 2004, at pp. 29-30, 48

28. However, the trial-level criminal case law is divided over whether IP address histories should receive s. 8 *Charter* protection. Some cases have recognized a reasonable expectation of privacy over this information and held that the police should need a warrant to obtain it from an ISP, while others – including the judgment on appeal – reach the opposite conclusion.[49] The decisions finding no reasonable expectation of privacy make three main analytic errors, discussed in detail below. The trial judge's reasons in the case at bar reveal several further errors.

c) Errors in the Decisions Finding No Reasonable Expectation of Privacy

(1) Mischaracterizing the Nature of the Information at Issue

29. The first recurring theme in these cases is the suggestion that all that is being disclosed is an ISP subscriber's name and street address, over which he or she has only a minimal privacy interest. For instance, the trial judge in the case at bar characterized the police request as "narrow and involv[ing] only [the Appellant's] name and address",[50] adding:

> Generally speaking, in modern day society, a person's name and address is used and shared frequently. A privacy issue is largely contextual in that a person may not want others to share information such as whether he or she is a subscriber to the services of an Internet Provider. [51]

Likewise, in *R. v. F.(S.W.), supra* Nadel J. stated:

> [A]ccount information, *per se*, reveals very little about the personal lifestyle or private decisions of the occupants of the defendant's residence other than they have chosen to have some form of Internet connection installed in that residence.[52]
>
> Ruling on *Charter* Motion, ¶59-67, *Appeal Book*, pp. 27-28

---

[49] See ¶13, *supra* and the cases cited at footnotes 11&12, *supra*.
[50] Ruling on *Charter* Motion, *supra* at ¶65.
[51] Ruling on *Charter* Motion, *supra* at ¶67.
[52] *R. v. F.(S.W.), supra* at ¶24; see also *R. v. Wilson, supra* at ¶42.

30. With respect, this mischaracterizes the information actually being revealed to the police in these cases. The police are not interested in knowing merely whether someone has a subscription with a particular ISP. Rather, they seek information that can reveal the web sites the subscriber has visited and his or her activities at these sites, which can in turn expose highly personal "core biographical information" about the subscriber. It is this privacy interest that is threatened by the disclosure of IP address histories, not merely the lesser interests associated with the existence of an Internet account or a street address. Further, this privacy interest must be assessed with regard to what the disclosed information *could* reasonably reveal, rather than by an *ex post facto* analysis considering only how the police actually used it in a particular case.

> *R. v. Cuttell*, *supra* at ¶21-27
> *Hunter v. Southam*, *supra* at p. 109

31. This mischaracterization has led some courts (including the trial judge in the case at bar) to rely on a flawed analogy between IP addresses and telephone numbers.[53] There are significant functional and practical differences between these types of numbers. Most importantly, disclosing telephone directory information does not expose a subscriber's calling history. Merely knowing someone's telephone number does not reveal with whom he or she has spoken or what they discussed. This latter information is generally accessible to the police only with judicial authorization. In contrast, Internet users have no guarantee that the places their IP addresses have visited will remain secret. Knowing the sites and web pages people have visited often reveals more about them than does the telephone numbers they have called.[54] Privacy in cyberspace thus depends on confidentiality being maintained over the ISP's records linking accounts to specific

---

[53] Specifically, the cases rely on *R. v. Edwards*, [1999] O.J. No. 3819 (S.C.J.), holding that a telephone subscriber has no reasonable expectation of privacy over the association between his or her identity and a particular telephone number.

[54] For example, if a person calls the Telehealth Ontario hotline this may support the inference that he or she has some kind of medical concern but does not reveal its exact nature. On the other hand, if the person visits a particular page on an Internet medical reference website this can reveal more intimate details about his or her interests.

IP addresses at specific times. Disclosure of these records threatens to reveal information that is not ordinarily exposed by disclosing a person's telephone number.[55] As Wilkins J. noted in *Irwin Toy Ltd. v. Doe, supra*, for this reason there is a general expectation that these records will be disclosed only when required by law.

(2) Mischaracterizing the Effect of Contractual Terms

32. The second recurring theme in the trial-level case law is the claim that subscribers' contractual terms with their ISPs erode their expectation of privacy over their IP address histories. The Bell Sympatico documents adduced in the case at bar did not specifically address the issue of disclosing subscribers' IP address histories to the police. Nevertheless, the trial judge relied on terms stating that Bell Sympatico would "disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction",[56] and would "offer full cooperation with law enforcement agencies in connection with any investigation" arising from a breach of Bell's "Acceptable Use Policy" ("AUP").[57] He concluded that "[t]he gist of the contractual information with Bell Sympatico was that personal information could, in certain circumstances, be shared with the police", and that Bell "had reserved the contractual right to disclose information especially in situations involving investigations of child pornography".[58]

---

[55] A better analogy can be drawn between IP address histories and detailed cell phone records revealing details of calls made and received and the physical location of the subscriber during these calls. These records have been found to attract a reasonable expectation of privacy because they reveal information that is "is readily translated into core biographical information": *R. v. Bryan*, 1999 CanLII 14911 at ¶15 (Ont. S.C.J.); see also *R. v. MacInnis, supra; R. v. Mahmood, supra*.

[56] Bell Sympatico Service Agreement, ¶17 [emphasis added], Affidavit of T. Burtt (Exhibit 2), *Appeal Book*, Tab 5B, p. 21.

[57] Bell Sympatico Internet Services – Acceptable Use Policy, Affidavit of T. Burtt (Exhibit 2), *Appeal Book*, Tab 5B, pp. 26, 28. Among other things, the AUP prohibited subscribers from using their accounts to access or download child pornography.

[58] Ruling on *Charter* Motion, *supra*, at ¶69. See also *R. v. F.(S.W.), supra*; *R. v. Wilson*, *supra; R. v. Vasic*, *supra*.

33. This approach stands the law on its head. Parliament enacted *PIPEDA* because it decided that consumer privacy should no longer be left to the marketplace. Businesses cannot contract out of their *PIPEDA* obligations, and terms they unilaterally insert into "contracts of adhesion" with consumers must be interpreted in light of these statutory duties. In particular, *PIPEDA* expressly prohibits businesses from disclosing personal information in response to a "governmental request" unless the "request" is backed up by "lawful authority".[59] The clause in Bell's Service Agreement authorizing it to disclose information "to satisfy … [a] governmental request" must be understood in light of this restriction, as must the clause in Bell's AUP authorizing "cooperation" with the police.[60] Likewise, these terms cannot reasonably be seen as eroding customers' expectations of privacy to such a degree that *Charter* protection is ousted.

> *Griffin v. Dell Canada Inc.* (2010), 98 O.R. (3d) 481 at ¶29 (C.A.)

34. It must also be borne in mind that few ISP subscribers can be expected to parse standard-form service contracts minutely and appreciate every potential nuance. As Deschamps J. observed in her plurality reasons in *R. v. Gomboc*, *supra* (at para. 33):

> [I]n view of the multitudinous forms of information that are generated in customer relationships and given that consumer relationships are often governed by contracts of adhesion … there is every reason for proceeding with caution when deciding what independent constitutional effect disclosure clauses similar to those in the [Alberta] *Code of Conduct Regulation* may have on determining a reasonable expectation of privacy.

The statutorily-created contractual terms in *Gomboc* were, as Abella J. noted in her concurring reasons, "clear and unambiguous": they authorized the utility to disclose <u>any</u> "customer information" to the police unless the customer had expressly requested otherwise. In contrast, Bell Sympatico <u>did not</u> expressly tell customers that their IP address histories would be disclosed on police requests, notwithstanding *PIPEDA*. Instead, its contractual documents repeatedly

---

[59] See ¶16ff, *supra*.

[60] It should also be noted that the wording of the RCMP letters of request in the case at bar did not specifically allege that any Bell Sympatico subscriber had violated the terms of the AUP or reveal anything beyond the bare fact that the police were "conducting an investigation in relation to child sexual exploitation offences".

assured customers their personal information would not be disclosed except as "required by law".[61] Subscribers who took the time to read these documents alongside *PIPEDA* and the *Charter* jurisprudence would not reasonably conclude that they were giving up their *Charter* right to insist that the police obtain a warrant in order to gain access to private information.

35. Whether or not a "reasonable expectation of privacy" should be recognized over particular information is fundamentally a normative question. If this Court is satisfied that IP address histories otherwise satisfy the criteria for s. 8 *Charter* protection, it is submitted that there is nothing in Bell Sympatico's contractual materials that demands a different result.

(3) Expectations of Privacy and Illegal Conduct

36. The third major theme in the "no expectation of privacy" decisions is the contention that ISP subscribers forfeit all privacy when they use the Internet unlawfully. For instance, in the case at bar the trial judge rested his conclusion that the Appellant had no reasonable expectation of privacy over his IP address history in part on the claim that he could not "claim a privacy interest in any illegal information he may have been accessing at the subject web site".[62] Nadel J. expanded on this argument in *R. v. F.(S.W.), supra*, stating:

> I find that the defendant had no reasonable expectation of privacy in account information respecting his illegal use of the internet service provided by Bell. … In my view he could have no reasonable expectation that customer account information respecting his internet use to distribute child pornography would remain confidential. [Underlining in original].[63]

37. This reasoning is contrary to binding Supreme Court of Canada *Charter* jurisprudence. In *R. v. Wong*, *supra*, the Court considered whether someone hosting an illegal gambling session in his hotel room thereby lost all reasonable expectation of privacy. Writing for the majority, La

---

[61] See, *e.g.*, "Service Agreement", *supra*, ¶13; *Bell Code of Fair Information Practices, Appeal Book*, pp. 38, 40.
[62] Ruling on *Charter* Motion, *supra* at ¶69, *Appeal Book*, p. 30.
[63] *R. v. F.(S.W.), supra* at ¶21. See also *R. v. McGarvie, supra* at ¶37.

Forest J. rejected the argument that privacy determinations could be based on "*ex post facto* reasoning" assuming the defendant's guilt, explaining:

> [I]t would be an error to suppose that the question that must be asked in these circumstances is whether persons who engage in illegal activity behind the locked door of a hotel room have a reasonable expectation of privacy. Rather, the question must be framed in broad and neutral terms so as to become whether in a society such as ours persons who retire to a hotel room and close the door behind them have a reasonable expectation of privacy.[64]

The Court recently reaffirmed this holding in *R. v. M.(A.), supra* and the companion judgment, *R. v. Kang-Brown*, where Deschamps J. (dissenting in the result, but not on this point) explained:

> When a court considers whether an accused had a reasonable expectation of privacy, the issue is not whether he or she was involved in criminal activity. As this Court stated in *Hunter v. Southam* [*supra*, at p. 109 C.C.C.], an *ex post facto* analysis to determine this would be at odds with the purpose of s. 8, which is to prevent unreasonable searches before they occur. Thus, to assess whether the expectation of privacy was reasonable, the court must first frame the alleged privacy interest in broad and neutral terms. [65]

Under this approach, the question in the case at bar is whether Internet subscribers *in general* should be entitled to privacy over information in their ISP's files that could reveal details of their Internet activities. The issue cannot be framed by assuming that everyone whose information is requested by the police must be guilty of an offence.

38. It also must be emphasized that the issue in this case <u>is not</u> what Bell Sympatico could have done if it had independently uncovered evidence of the Appellant's wrongdoing. If Bell employees had discovered that the Appellant was using his account to access child pornography and had reported this to the police, he would probably have had no grounds for complaint under either *PIPEDA* or the *Charter*.[66] However, that is not what happened here. There is no indication that Bell Sympatico ever suspected the Appellant of misusing his account before it received the

---

[64] *R. v. Wong*, *supra*, at p. 481.

[65] *R. v. Kang-Brown*, 2008 S.C.C. 18, 230 C.C.C. (3d) 289 at ¶138; *R. v. M.(A.), supra* at ¶70-74. See also *R. v. Buhay*, *supra* at 19; *R. v. Mercer*, *supra* at p. 185.

[66] In this situation Bell's disclosure of information to the police would have been authorized by *PIPEDA* s. 7(*d*)(i), which permits disclosures "on the initiative of [an] organization to an investigative body" when the organization "has reasonable grounds to believe that the information relates to … a contravention of the laws of Canada". Likewise, in this scenario the disclosure would not have violated the Appellant's *Charter* rights because Bell Sympatico would not have been acting as a state agent.

RCMP requests.[67] Rather, Bell disclosed information about the Appellant entirely in response to these police requests. The Appellant's privacy interest over this information was not diminished by the mere possibility that in different circumstances it might have been disclosed by non-state actors – a risk that never actually materialized.

R. v. Buhay, supra at ¶32-40
R. v. Wong, supra

(4) Other Analytic Errors by the Trial Judge

39. The trial judge's reasons in the case at bar reveal several further analytic errors. First, he incorrectly treated the possibility that the police could have obtained a warrant to seize the Appellant's IP address history from Bell Sympatico as supporting the conclusion that this information was not private.[68] Search warrants *override* reasonable expectations of privacy, not negate them. A search conducted pursuant to lawful warrant is still a "search" for s. 8 purposes, albeit a "reasonable" one. The prospect of warrant issuing here simply had no bearing on the threshold question of whether the information in question was private and protected by s. 8.

40. The trial judge erred further by citing the Appellant's apparent efforts to conceal his identity as a factor weighing against his having any expectation of privacy over his Internet activities.[69] He reasoned that if the Appellant "had not attempted to disguise his identity as a website user" his true identity "may have been more easily attainable", and cited this as a factor supporting his conclusion that the Appellant lacked any reasonable expectation of privacy. The underlying logic of this argument is difficult to discern. The Appellant's active efforts to

[67] It should also be noted that the RCMP "letters of request" did not specifically accuse the person assigned the listed IP addresses of any wrongdoing. Rather, they merely stated that the police were investigating "child sexual exploitation offences under the *Criminal Code*". The fact that the police were interested in certain IP addresses did not necessarily imply that these addresses had themselves been used illegally or contrary to the subscribers' service contract. For instance, it was entirely possible that the police were seeking to identify a person who had posted a comment on a web site claiming to have witnessed a child sexual offence.
[68] Ruling on *Charter* Motion, ¶69, *Appeal Book*, p. 29.
[69] Ruling on *Charter* Motion, ¶69, *Appeal Book*, p. 29.

preserve his anonymity *supported* his claim that he at least subjectively expected his online activities to remain private. The key question was whether this expectation was reasonable in the circumstances as they actually existed. This question could not be answered on the basis of counterfactuals in which the Appellant was assumed to have done exactly the opposite of what he actually did.

B. Issue 2: The Issuance of the Search Warrant for the Appellant's Home and Computers

41. If the information from Bell Sympatico was obtained unconstitutionally it must be excised from the subsequent search warrant application regarding the Appellant's home.[70] Without this information the police had no grounds even to suspect the Appellant and the warrant could not have issued.

42. In the alternative, even if the Bell Sympatico information was lawfully obtained, it is submitted that there were insufficient grounds to support the issuance of the warrant. The trial judge ruled on this issue without the advantage of the Supreme Court of Canada's subsequent decision in *R. v. Morelli, supra,* which undercuts his conclusions in two critical respects. First, after *Morelli* the evidence in DC Burtt's ITO can no longer be seen as raising reasonable grounds to believe the Appellant had committed the offence of possessing child pornography (as distinct from the separate "accessing" offence). Second, and even more significantly, *Morelli* fatally undermines the police claim that they had reasonable grounds to believe that a search of the Appellant's home in May, 2007 would reveal evidence of either offence.

> Ruling on *Charter* Motion, ¶71-111, *Appeal Book*, pp. 17-37
> *R. v. Morelli, supra* at ¶5-9, 13-38, 62-97

[70] See *R. v. Plant, supra* at p. 211, *R. v. Grant* (1993), 84 C.C.C. (3d) 173 at p. 195 (S.C.C.); *R. v. Wiley* (1993), 84 C.C.C. (3d) 161 at p. 169 (S.C.C.).

43. *Morelli* makes two critical holdings. First, the majority decision establishes that a computer user does not "possess" child pornography merely by viewing images online, even though this causes the underlying data files to be automatically downloaded to the user's hard drive.[71] This has immediate implications for search warrant applications:

> Plainly, the mere fact that an image has been accessed by or displayed in a Web browser does not, without more, constitute possession of that image. An ITO seeking a warrant to search for evidence of possession (rather than accessing) must therefore provide reasonable and probable grounds to believe that the alleged offender possesses (or has possessed) digital files of an illegal image, and that evidence of that possession will be found in the place to be searched. It is not enough to provide reasonable and probable grounds to believe that the alleged offender viewed or accessed illegal images using a computer, without knowingly taking possession — which includes control — of the underlying files in some way. [Emphasis added.][72]

Second, *Morelli* holds that the police cannot rely exclusively on "unsupported generalizations about the propensities of certain 'types of offenders' to hoard and copy illegal images"[73] in order to raise reasonable grounds that evidence will be found in the place searched. Instead, the police must establish on evidence both that there is actually some identifiable class of offenders with this propensity, and that the target of the search belongs to this group.

> *R. v. Morelli, supra* at ¶12-38, 62-97

44. On the facts of *Morelli* Fish J., writing for the majority, concluded that neither requirement was met. He agreed that the police had reasonable grounds to believe the defendant had accessed child pornography several months earlier by "brows[ing] a Web site that contained explicit images of females under the age of 18".[74] However, he held that it *could not* reasonably be inferred from this that the defendant had intentionally downloaded and saved any image files, or that there were reasonable grounds to believe illegal images would *now* be found in his home. Accordingly, the search warrant was quashed and the seized evidence excluded. Fish J. noted

---

[71] See *Morelli, supra* at ¶12-38.
[72] *Morelli, supra* at ¶31.
[73] *Morelli, supra* at ¶70; see also ¶63, 69-97.
[74] *Morelli, supra* at ¶64. Specifically, he concluded that this inference could be drawn from the titles of some web browser "bookmarks" a technician had observed on the accused's computer "desktop".

that the jurisprudence does not "support the notion that a warrant can be issued months after a person might have merely viewed child pornography."[75]

R. v. Morelli, supra at ¶62-97
R. v. Fawthrop (2002), 161 O.A.C. 350

45. It is submitted that the principles established in *Morelli* demand the same result on the facts of the case at bar. There are two potentially relevant factual differences which must be acknowledged and addressed. First, unlike the police in *Morelli* the police in the case at bar sought a warrant in relation to both the offences of possession *and* accessing. Second, in *Morelli* the police specifically knew that the defendant's hard drive had been formatted some four months earlier, wiping out any saved data. The police in the case at bar did not have similar knowledge. However, on a closer examination neither of these differences materially change the analysis or the end result.

R. v. Morelli, supra at ¶6, 12, 31, 68

46. Although DC Burtt's ITO referred to both the possession and accessing offences, his application ultimately stood or fell on the strength of the claim that the Appellant probably had a collection of child pornography stored in his home. Significantly, DC Burtt did not suggest that he believed the search would reveal direct evidence of the three occasions in June and July, 2006 – almost eleven months earlier – when the Appellant's ISP account had accessed seven unlawful images over a 26-second period. Although he stated that "[d]eleted files or file fragments may exist for an extended period of time (e.g., weeks or months)" on a computer hard drive, he did not assert a belief that evidence of these particular accessing incidents would still be found on the Appellant's computer system at this late date. Rather, the central thrust of DC Burtt's

[75] *R. v. Morelli, supra* at ¶87.

application[76] was indistinguishable from that in *Morelli*: he relied on generalizations about the propensity of child pornography collectors to hoard images in their homes to support the inference that *the Appellant* probably kept such a collection in his home. In *Morelli* the majority rejected this approach, stating:

> [A]n evidentiary basis is required to support a finding as to the characteristics or propensities of child pornography offenders. An evidentiary basis is required as well for a finding of reasonable and probable grounds to believe that the alleged offender belongs to the class of child pornography offenders whose characteristics or propensities are mentioned in the ITO.[77]

47. As in *Morelli*, DC Burtt's ITO was deficient on both points. While his description of the alleged habits of child pornography collectors was somewhat longer than that in the *Morelli* ITO, it was similarly devoid of meaningful content. Even more importantly, DC Burtt's ITO presented no evidence to support the inference that *the Appellant* was a child pornography collector, other than the evidence indicating that his account had briefly accessed illicit images many months earlier. In *Morelli*, Fish J. concluded:

> [I]t cannot be assumed, without evidence, that broad but meaningful generalizations can be made about all persons who commit (or are suspected of committing) child pornography offences.
>
> …
>
> Two suspiciously-labelled links in the "Favourites" menu do not suffice to characterize a person as an habitual child pornography offender of the type that seeks out and hoards illegal images.[78]

Similarly, even if it could reasonably be inferred in the case at bar that the Appellant had on three occasions almost eleven months earlier accessed seven illicit images over a 26-second period, the evidence did not reasonably support the further inference that he was "an habitual child pornography offender of the type that seeks out and hoards illegal images".

ITO, *supra*, ¶155-65, *Appeal Book*, Tab 2C, pp. 49-50

---

[76] DC Burtt's ITO also contains what appear to be boilerplate paragraphs suggesting that the search might reveal evidence that the Appellant had *distributed* child pornography by creating an illegal web page or seeking "advice on how to build a web page or suggestions for what to put on it" (see, *e.g.*, ITO, ¶144-45). However, the police had no evidence whatsoever supporting the belief that the Appellant had ever hosted a child pornography web site or otherwise distributed illicit images.

[77] *R. v. Morelli*, *supra* at ¶80, 82.

[78] *R. v. Morelli*, *supra* at ¶77, 86.

48. In *Morelli*, the police sought a search warrant four months after the last known occasion when the accused might have accessed illicit images, knowing that his hard drive had been formatted during the intervening time. The passage of time in the case at bar had similar implications for the likelihood of finding evidence at the time of the search. The trial judge failed to appreciate why this delay was important, dismissing its significance on the grounds that "the investigation itself did not lie dormant".[79] With respect, this misses the point. The issue was not whether the police had been dilatory, but the impact of the delay on the prospects of the search bearing fruit. Stripped to its essentials, the search warrant application here ultimately depended on strength of the inference that the Appellant fit the profile of a child pornography collector who was unlikely to "destroy or delete [his] collection". After *Morelli*, this inference is no longer supportable.[80] On the evidentiary record here, the search warrant should not have been issued.

C. Issue 3: Section 24(2) *Charter* Exclusion of Evidence

49. Under the Supreme Court of Canada's "revised approach" to the s. 24(2) exclusion of evidence in *R. v. Grant, infra*, courts must consider and balance three factors: (i) the seriousness of the *Charter*-infringing state conduct; (ii) the impact of the breach on the accused's protected interests; and (iii) society's interest in an adjudication on the merits. However, the analysis cannot be reduced to simple "best two out of three" arithmetic: strength in one factor can tip the balance in favour of admission or exclusion even when the other two factors support the opposite result but do so less strongly.

R. v. Grant, 2009 S.C.C. 32, 245 C.C.C. (3d) 1 at ¶67-140

50. The evidence seized from the Appellant's home was reliable and essential to the Crown's case, factors tending to favour its admission. On the other hand, the searches of the Appellant's

[79] Ruling on *Charter* Motion, ¶105, *Appeal Book*, p. 36.
[80] The Crown cannot, of course, rely on *ex post facto* justification based on the fact that the search in this case in fact did reveal evidence.

home and computer were highly invasive and significantly intrude on his right to privacy. As Fish J. stated in *Morelli, supra*:

> [I]t is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.
>
> It is therefore difficult to conceive a s. 8 breach with a greater impact on the *Charter*-protected privacy interests of the accused than occurred in this case. [81]

The second *Grant* factor thus weighs strongly in favour of exclusion.

51. The first *Grant* factor requires a consideration of the good faith, or lack thereof, of the investigating officer. If the warrantless police request for information from Bell Sympatico is found to violate s. 8 of the *Charter*, consideration must be given to the conduct of the RCMP officer who made the request. At the time of the request, the police were operating in an area of some legal uncertainty. However, the jurisprudence at the time supported the view that the information at issue was private and protected by s. 8 of the *Charter*.[82] The RCMP chose to ignore this jurisprudence and take an expansive view of their powers under *PIDEDA*. If they were wrong, their error cannot be characterized as a mistake good faith.

52. If the RCMP request to Bell Sympatico is found to have been lawful, the focus must shift to the actions of the Sudbury police who sought and executed the search warrant. Unlike the police in *Morelli*, the Sudbury officers did not misstate the relevant facts in a manner that would have significantly misled the issuing justice, and cannot in this sense be accused of "bad faith". At the same time, they should have recognized that by May, 2007 their grounds for believing evidence would be found in the Appellant's home had grown extremely stale. Accordingly, while the first *Grant* factor may tend to favour admission, it does so only weakly. On balance, it

---

[81] *R. v. Morelli, supra* at ¶105-06.
[82] See *BMG Canada v. Doe, supra*; *Irwin Toy v. Doe, supra; Re S.(C.), supra*.

is submitted that having regard to the extremely serious impact of the search on the Appellant's privacy rights, if the warrant in this case should not have been issued the administration of justice would be brought into greater disrepute by admitting the evidence than by its exclusion.

PART IV: ORDER REQUESTED

53. It is respectfully submitted that the appeal be allowed and an acquittal entered or, in the alternative, a new trial ordered.

ALL OF WHICH IS RESPECTFULLY SUBMITTED THIS 31st DAY OF JANUARY, 2011

_____
JONATHAN DAWE
SACK GOLDBLATT MITCHELL LLP
20 Dundas St. West, Suite 1100
Toronto, Ontario
M5G 2G8

OF COUNSEL FOR THE APPELLANT

APPELLANT'S TIME ESTIMATE FOR ORAL ARGUMENT: 1½ HOURS

PART V: AUTHORITIES TO BE CITED

Personal Information Protection and Electronic Documents Act ("PIPEDA"), S.C. 2000, c. 5

R. v. Cuttell (2009), 247 C.C.C. (3d) 424 (Ont. C.J.)

R. v. Garbett, 2008 ONCJ 97, *aff'd* 2010 ONSC 2762

R. v. Morelli, 2010 SCC 8, 282 C.C.C. (3d) 273

R. v. Kwok, [2008] O.J. No. 2414 (S.C.J.)

Re C.(S.), [2006] O.J. No. 3754 (C.J.)

R. v. F.(S.W.), 2008 ONCJ 740

R. v. Wilson, 2009 O.J. No. 1067 (S.C.J.)

R. v. Vasic, 2009 CanLII 6842 (Ont. S.C.J.)

R. v. McGarvie, 2009 CarswellOnt 500 (C.J.)

R. v. Verge, 2009 CarswellOnt 501 (C.J.)

R. v. Brousseau, 2010 ONSC 6753

R. v. Trapp, 2009 SKPC 5

R. v. McNeice, 2010 BCSC 1544

R. v. Tessling, 2004 S.C.C. 67, 189 C.C.C. (3d) 129

R. v. Plant (1993), 84 C.C.C. (3d) 203 (S.C.C.)

R. v. Law 2002 S.C.C. 10, 160 C.C.C. (3d) 449

R. v. Wills (1992), 70 C.C.C. (3d) 529 (Ont. C.A.)

R. v. Dyment (1988), 45 C.C.C. (3d) 244 (S.C.C.)

R. v. Wong (1990), 60 C.C.C. (3d) 460 (S.C.C.)

R. v. Mercer (1992), 70 C.C.C. (3d) 180 (Ont. C.A.)

R. v. Buhay (2003), 174 C.C.C. (3d) 97 (S.C.C.)

R. v. Collins (1987), 33 C.C.C. (3d) 1 (S.C.C.)

Hunter v. Southam Inc. (1984), 14 C.C.C. (3d) 97 (S.C.C.)

R. v. M.(A.) (2008), 230 C.C.C. (3d) 377 (S.C.C.)

R. v. Patrick, 2009 SCC 1, 242 C.C.C. (3d) 158

R. v. Gomboc, 2010 S.C.C. 55

R. v. Wong (1990), 60 C.C.C. (3d) 460 (S.C.C.)

United States v. Katz, 389 U.S. 347 (1967)

R. v. Lubovac (1989) 52 C.C.C. (3d) 551 (Alta. C.A.)

R. v. Solomon (1992), 77 C.C.C. (3d) 264 (Que. Mun. Ct.)

R. v. Solomon (1993), 85 C.C.C. (3d) 496 at pp. 509-18 (Que. Mun. Ct.); *rev'd on other grounds* (1996) 110 C.C.C. (3d) 354 (Que. C.A.), *aff'd* (1997), 118 C.C.C. (3d) 351 (S.C.C.)

R. v. Edwards (1996), 104 C.C.C. (3d) 136 (S.C.C.)

Schreiber v. Canada (Attorney General) (1998), 124 C.C.C. (3d) 129 (S.C.C.)

R. v. Lillico (1994), 92 C.C.C. (3d) 90 (Ont. Gen. Div.), *aff'd* 1999 CanLII 2836 (Ont. C.A.)

R. v. Quinn (2006), 209 C.C.C. (3d) 278 (B.C.C.A.)

R. v. D'Amour (2002), 166 C.C.C. (3d) 477 (Ont. C.A.)

R. v. Stymiest, 2006 N.B.Q.B. 160

R. v. Chusid (2001), 57 O.R. (3d) 20 (S.C.J.)

R. v. Eddy, 1994 CanLII 5274 (Nfld. S.C.T.D.)

R. v. Weir (2001), 156 C.C.C. (3d) 188 (Alta. C.A.)

R. v. MacInnis 2007 CanLII 29342 (Ont. S.C.J.);

R. v. Mahmood (2008), 236 C.C.C. (3d) 3 (Ont. S.C.J.)

R. v. Pal and Tahvili, 2007 BCSC 1494

R. v. Lee, 2007 ABQB 767

Public Interest Advocacy Centre, *Consumer Privacy and State Security: Losing our Balance*, November, 2004

BMG Canada Inc. v. Doe, 2005 FCA 193

Irwin Toy Ltd. v. Doe, [2000] O.J. No. 3318 (S.C.J.)

Warman v. Fournier et al., 2010 ONSC 2126

R. v. Edwards, [1999] O.J. No. 3819 (S.C.J.)

R. v. Bryan, 1999 CanLII 14911 (Ont. S.C.J.)

Griffin v. Dell Canada Inc. (2010), 98 O.R. (3d) 481 (C.A.)

R. v. Kang-Brown, 2008 S.C.C. 18, 230 C.C.C. (3d) 289

R. v. Grant (1993), 84 C.C.C. (3d) 173 (S.C.C.)

R. v. Wiley (1993), 84 C.C.C. (3d) 161 (S.C.C.)

C-50206

COURT OF APPEAL FOR ONTARIO

B E T W E E N:

HER MAJESTY THE QUEEN

Respondent

- and -

DAVID WARD

Appellant

APPELLANT'S FACTUM

JONATHAN DAWE
SACK GOLDBLATT MITCHELL LLP
20 Dundas Street West, Suite 1100
Toronto, Ontario
M5G 2G8

Tel: 416-977-6447
Fax: 416-591-7333
E-mail: jdawe@sgmlaw.com

COUNSEL FOR THE APPELLANT