Court File No: 34268

Publication Ban

Interdiction de publication

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

B E T W E E N :

HER MAJESTY THE QUEEN

Appellant

- AND -

RICHARD COLE

Respondent

- AND -

DIRECTOR OF PUBLIC PROSECUTIONS, ATTORNEY GENERAL OF QUEBEC, CRIMINAL LAWYERS' ASSOCIATION (ONTARIO), CANADIAN CIVIL LIBERTIES ASSOCIATION and CANADIAN ASSOCIATION OF COUNSEL TO EMPLOYERS

Interveners

RESPONDENT'S FACTUM

(pursuant to Rules 36 and 42 of the *Rules of the Supreme Court of Canada*)

FRANK ADDARIO
Addario Law Group
171 John Street, Suite 101
Toronto, ON M5T 1X3

T: 416.979.6446
F: 1.866.714.1196
Email: faddario@addario.ca

GERALD CHAN
NADER R. HASAN
Ruby Shiller Chan, Barristers
11 Prince Arthur Ave.
Toronto, ON M5R 1B2

T: 416.964.9664
F: 416.964.8305

Counsel for the Respondent,
Richard Cole

COLLEEN BAUMAN
Sack Goldblatt Mitchell LLP
30 Metcalfe Street, Suite 500
Ottawa, ON K1P 5L4

T: 613.235.5327
F: 613.235.3041
Email: cbauman@sgmlaw.com

Agent for the Respondent,
Richard Cole

JONATHAN C. LISUS
MICHAEL PERLIN
Lax O'Sullivan Scott Lisus LLP
145 King Street West
Suite 1920
Toronto, ON M5H 1J8

T: 416.598.1744
F: 416.598.3730
Email: jlisus@counsel-toronto.com

Counsel for the Intervener,
Canadian Civil Liberties Association

HENRY S. BROWN, Q.C.
Gowling Lafleur Henderson LLP

160 Elgin Street
Suite 2600
Ottawa, ON K1P 1C3

T: 613.233.1781
F: 613.563.9869
Email: henry.brown@gowlings.com

Agent for the Intervener,
Canadian Civil Liberties Association

DANIEL MICHALUK
Hicks Morley Hamilton Stewart Storie LLP
77 King Street West, 39th Floor
Box 371, TD Centre
Toronto, ON M5H 1K8

T: 416.864-7253
F: 416.362-9680
Email: daniel-michaluk@hicksmorley.com

Counsel for the Intervener,
Canadian Association of Counsel to Employers

SIOBHAN O'BRIEN
Hicks Morley Hamilton Stewart Storie LLP
150 Metcalfe Street
Suite 2000
Ottawa, ON K2P 1P1

T: 613.369.8411
F: 613.234.0418
Email: siobhan-obrien@hicksmorley.com

Agent for the Intervener,
Canadian Association of Counsel to Employers

DOMINIQUE A. JOBIN
Procureur général du Québec
1200, route de l'Église, 2e étage
Sainte-Foy, QC G1V 4M1

T: 418.643.1477, ex. 20788
F: 418.644.7030
Email: djobin@justice.gouv.qc.ca

Counsel for the Intervener,
Attorney General of Quebec

PIERRE LANDRY
Noël & Associés
111, rue Champlain
Gatineau, QC J8X 3R1

T: 819.771.7393
F: 819-771-5397
Email: p.landry@noelassocies.com

Agent for the Intervener,
Attorney General of Quebec

TABLE OF CONTENTS

PART I – OVERVIEW AND FACTS

A. Overview

1. In *Morelli*, this Court held that "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer." In this case, the Crown appeals against the exclusion of evidence arising from a warrantless search. The appeal raises the following question: Is there a reasonable expectation of privacy in the contents of a workplace computer distributed by the Respondent's employer?

2. The Crown says no. For the Crown's appeal to succeed it must persuade the Court to reverse a long line of jurisprudence that says that s. 8 of the *Charter* protects privacy, and not property. It must persuade the Court to reverse its own cases holding that the police cannot piggyback on the authority of a third party to invade privacy. Finally, it must convince the Court to introduce the controversial American "assumption of risk" doctrine into our s. 8 *Charter* jurisprudence.

3. The Crown's appeal should be dismissed. The Respondent enjoyed a reasonable expectation of privacy in his work computer. Even if his employer enjoyed a right of access to the computer, the police did not. The police searches of the Respondent's computer were unreasonable. They were executed without warrant, without consent, and without exigent circumstances. Moreover, they were overbroad in scope. The evidence obtained in violation of the Respondent's s. 8 rights was correctly excluded under s. 24(2) of the *Charter*. All the police had to do in this case was get a warrant. This would not have prejudiced their investigation in the slightest. They chose not to do so.

B. Factual Background

4. The Respondent was a teacher "of long-standing and good reputation," who taught communications technology at a high school in the Rainbow District School Board (the "School Board"). In addition to his teaching duties, he had supervisory duties with respect to the operation of the school's computer network. The Respondent had domain administrative rights, which enabled him to access the server and all computers using the server within the school.

Ruling on *Charter* Motion, Guay J. Ont. Ct., May 12, 2008 [hereinafter "*Charter* Ruling"], A.R., Vol. I, pp. 5:29-5:30, 6:3-6:10, 29:27

5. The School Board issued the Respondent a laptop. Laptops were available to many of the teachers and staff at the school. The Respondent's use of the laptop was exclusive and such exclusive use was secured by a password.

Charter Ruling, A.R., Vol. I, p. 21:20-21:42

6. On June 23, 2006, a school technologist, Ryan Taggart, who had access to all computers on the school network, accessed the Respondent's computer "E" drive. Mr. Taggart was not asked to do so by any of his superiors. Rather, he did so as part of his role of "facilitating" the school's server and keeping "an eye out for problems."

Charter Ruling, A.R., Vol. I, p. 6:20-6:28

7. In the process of searching the Respondent's computer, Mr. Taggart discovered what he believed to be pornographic images of a student at the school. The photographs depicted a young woman posing nude or partially nude.[1] It was later discovered that the young woman was a student who had sent the photographs to her then-boyfriend (another student at the school) and that the Respondent had copied the photographs from that student's computer.

Charter Ruling, A.R., Vol. I, p. 8:10

8. On the following Monday, Mr. Taggart met with the school principal, Bruce Bourget, and disclosed what he had found. After confirming that the photographs did in fact depict a student at the school, Principal Bourget ordered Mr. Taggart to copy the photographs onto a compact disc, which he took into his possession. Principal Bourget then sought direction from the superintendents at the School Board. He was advised to get statements from all who had knowledge of the pictures and to seize the Respondent's laptop when he came to school.

Charter Ruling, A.R., Vol. I, pp. 8:24, 9:10-9:19

---

[1] The Crown describes these photographs as "extremely explicit." (Appellant's Factum, para. 11) None of the courts below or the witnesses characterized the photographs in this way. Principal Bourget described the photographs as being of a "young female … in various poses" and said that some of the photographs "were partially clothed and some were nude shots." *See* Evidence of Bruce Bourget, A.R., Vol. II, pp. 26:26-27:2.

9. When the Respondent arrived at school the next morning, Principal Bourget confronted the Respondent about inappropriate material being found on the laptop and demanded that the Respondent turn over his laptop. The Respondent complied with Principal's demand. But when Principal Bourget requested the Respondent's computer password, he refused to provide it.

Charter Ruling, A.R., Vol. I, p. 10:3-10:4

10. Although the Respondent's laptop had been provided by the School Board, the Respondent was permitted to and did in fact use it for personal activities. The Respondent had stored on the laptop images of his wife, his family's tax returns and other personal financial information. Upon surrendering his laptop, the Respondent told the Principal that he had photographs of his wife on the computer and pleaded that these photographs not be accessed.

Affidavit of Michael Venture, A.R., Vol. I, p. 107

Reasons for Judgment, Court of Appeal, March 22, 2011 ["Court of Appeal Judgment"], A.R., Vol. I, p. 83, para. 86

11. Principal Bourget provided the computer to the School Board. Despite not having the password, School Board technicians were able to bypass the password and access the computer. The technicians copied the temporary Internet files, which captured the Respondent's Internet browsing history, from the Respondent's laptop onto a compact disc.

Charter Ruling, A.R., Vol. I, p. 10:3-10:4

12. The following day, an officer of the Greater Sudbury Police Service (the "Sudbury Police"), D.C. Burtt, seized the disc with the photographs, the disc with the temporary Internet files, and the Respondent's laptop. D.C. Burtt viewed the files immediately upon seizure and then immediately sent the entire laptop for forensic analysis. He did not obtain a warrant.

Charter Ruling, A.R., Vol. I, pp. 10:25-11:3

13. D.C. Burtt was an experienced officer assigned to the Cyber-Crime Unit of the Sudbury Police. He had been working in the area of cyber-crime since November 2002. He had received extensive specialized training in this area through the Canadian Police College and the Ontario Police College as well as civilian agencies that provide computer and Internet-related training.

He had also attended a course at the Ontario Police College for specialized training in search warrants.

Charter Ruling, A.R., Vol. I, pp. 10:25-11:3
Evidence of Timothy Burtt, A.R., Vol. II, pp. 111:12-111:28, 113:5

14. D.C. Burtt acknowledged that he was aware that teachers at the Respondent's school were permitted to use their laptops for personal use and that they may have "sensitive personal information" on the laptops. Indeed, prior to sending the Respondent's laptop for forensic analysis without a warrant, D.C. Burtt was provided with a letter written by a teacher to Principal Bourget, which explained that teachers may have sensitive personal information such as bank account numbers and personal financial information as well as information about their students on their laptops. When asked whether he had considered getting a warrant at any stage of the proceedings, D.C. Burtt testified that because the laptop belonged to the School Board, there was no need for him to get a warrant.

Evidence of Timothy Burtt, A.R., Vol. II, pp. 126:16-127:4, 155:20-155:26
Copy of letter dated June 27, 2006 from Daryl Smith to Bruce Bourget, A.R., Vol. II, pp. 219-220
Charter Ruling, A.R., Vol. I, p. 11:10-11:15

C. Procedural History

15. After conducting a *voir dire,* the trial judge found that the searches of the Respondent's laptop by the Sudbury Police violated s. 8 of the *Charter*. As a result, the trial judge excluded the evidence seized by the police and acquitted the Respondent. Relying on this Court's opinion in *Buhay*, the trial judge held that the Respondent enjoyed a reasonable expectation of privacy in his work computer, which "was on par with an office desk or a rented locker at least." Therefore, the police could not, absent a warrant, execute a reasonable search and seizure of the compact disc containing the photographs and the Internet files, or the Respondent's laptop. D.C. Burtt was an experienced cyber-crime officer who "by-pass[ed] the constitutional route to obtain the evidence" despite the fact that obtaining a warrant would not have prejudiced the investigation. Therefore, this was an "egregious breach" that justified exclusion under s. 24(2).

Charter Ruling, A.R., Vol. I, pp. 22:11-22:13, 28:14-28:25, 31:3-31:20

16. The Superior Court of Justice granted the Crown's summary conviction appeal, holding that the Respondent had no reasonable expectation of privacy in his work computer. The Superior Court's decision turned in large part on one of the school policies — the Acceptable Use Policy ("AUP") — and the applicability of that policy to teachers as well as students.

> Reasons for Judgment, Superior Court of Justice, April 28, 2009 ["Superior Court Judgment"], A.R., Vol. I, p. 42

17. The Court of Appeal for Ontario granted the Respondent's appeal. Justice Karakatsanis (as she then was), writing for a unanimous Court, held that the Respondent had a reasonable expectation of privacy from state intrusion in the personal use of his work computer and in the contents of his personal files on its hard drive. There was "no clear privacy policy relating to teachers' laptops" and while the laptop was owned by the School Board, the Respondent "in fact had exclusive use and possession of the laptop and protected access to the laptop by use of a password." Because the Respondent had a reasonable expectation of privacy in the contents of his laptop, the police search and seizure without a warrant was presumptively unreasonable and the Crown failed to rebut this presumption. The Court held, however, that different considerations applied to the disc containing the photographs of the student as these images were in "plain view" of the technician who was doing routine maintenance of the network. Thus, the Court of Appeal excluded the laptop and the disc containing the temporary Internet files, but not the disc containing the photographs of the student.

> Court of Appeal Judgment, A.R., Vol. I, p. 50, para. 6; pp. 53-54, para. 16; p. 61, paras. 38-39; p. 79, paras. 79-80; pp. 82-83, paras. 85-87

PART II – POSITIONS ON APPELLANT'S QUESTIONS

Issue One: The Respondent's reasonable expectation of privacy should be assessed on the totality of the circumstances, which supports a reasonable expectation of privacy in this case.

Issue Two: The warrantless search and seizure of the computer evidence by the police was presumptively unreasonable and the Crown has failed to rebut that presumption.

Issue Three: The Court of Appeal correctly excluded the computer evidence.

PART III – STATEMENT OF ARGUMENT

I. THE RESPONDENT HAD A REASONABLE EXPECTATION OF PRIVACY IN THE CONTENTS OF HIS SCHOOL LAPTOP

18. The State infringes s. 8 of the *Charter* where it interferes with one's reasonable expectation of privacy. The existence of a reasonable expectation of privacy is determined by considering the "totality of the circumstances." The first step is to determine whether the Respondent had a subjective expectation of privacy in the informational content in his laptop. If so, this Court must then decide whether that subjective expectation was objectively reasonable.

Hunter v. Southam, [1984] 2 S.C.R. 145 at 159-160
R. v. Patrick, [2009] 1 S.C.R. 579 at para. 27
R. v. Tessling, [2004] 3 S.C.R. 432 at para. 32

A. The Respondent Had a *Subjective* Expectation of Privacy

19. It is beyond dispute that the Respondent had a subjective expectation of privacy in the informational content on the laptop. He appreciated that he had no ownership right in the computer, but maintained a privacy interest in the information stored on it. The Respondent had sole possession and exclusive use of the computer, with "such exclusive use being secured by a password." Further, the Respondent was permitted to and did in fact use the laptop for personal tasks. The Respondent stored images of his wife, tax returns and other personal financial information on the computer. As stated in *Little*, given "the personal nature of the material on the [computer], a subjective expectation of privacy can be presumed."

Court of Appeal Judgment, A.R., Vol. I, p. 83, para. 86
R. v. Little, [2009] O.J. No. 3278 at para. 126 (S.C.J.)

20. The Respondent's actions were consistent with this subjective expectation. Notably, when Principal Bourget demanded that the Respondent surrender his laptop and provide his password, the Respondent provided the laptop but refused to surrender the password.

Charter Ruling, A.R., Vol. I, pp. 21:20-21:42, 22:20-22:25

B. The Respondent's Subjective Expectation of Privacy Was *Objectively* Reasonable

21. In *Edwards*, the Court identified a number of relevant factors to consider in determining whether a claimant's expectation of privacy is objectively reasonable. Consistent with the instruction in *Hunter v. Southam* to avoid "the austerity of tabulated legalism", the *Edwards* framework has frequently been used to meet the challenges posed by technological innovation. Significantly, the Court has always been mindful of the fact that reasonableness under s. 8 of the *Charter* represents a "normative rather than a descriptive standard". The task is to determine how much privacy Canadians *should* have, and not merely to catalogue how much privacy they currently enjoy.

> *R. v. Edwards*, [1996] 1 S.C.R. 128 at para. 45
>
> *Hunter v. Southam*, *supra* at 156
>
> *R. v. Tessling*, *supra* at paras. 32, 42
>
> Dawe, Jonathan, *et al.*, ""We don't need no stinking badges" – or Search Warrants, or Reasonable Grounds, For That Matter: Reasonable Expectations of Privacy in the 21st Century" (Paper presented to the CLA Fall Conference, 9-10 December 2011) [unpublished]

22. The following considerations underline an objectively reasonable expectation of privacy on the facts of this case:

(1) The fact that this is a computer search is the starting point. Computers and similar electronic devices are ubiquitous in modern life.

(2) Section 8 protects privacy, not property.

(3) The information over which privacy is asserted in this case — including data, photographs and documents stored on a laptop — lies at the "biographical core" of privacy.

(4) Employees do not check their privacy at the workplace door.

(5) The workplace policies at the school and School Board, as modified by custom and practice, permitted personal use of the workplace computer.

(6) Teachers do not have a diminished expectation of privacy in the school setting.

(7) The police cannot piggy back on a third party's right of access to circumvent the constitutional requirements of s. 8.

1. The Hard Drive for the Analysis

23. It is inarguable that absent strong constitutional protections, technology has the potential "to annihilate privacy." Modern computers, mobile phones, smart phones and personal digital assistants pose a unique challenge to s. 8 of the *Charter* because they defy easy analogy to the traditional sites of searches and seizures. As one law professor has commented, "Computers are like containers in a physical sense, homes in a virtual sense, and vast warehouses in an informational sense."

R. v. Wong, [1990] 3 S.C.R. 36 at 47

Kerr, Orin S., "Searches and Seizures in a Digital World" (2006) 119 Harv. L. Rev. 531 at 533

24. Therefore, as Justice Fish observed in *Morelli*, "it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer." The unimaginable "intrusiveness" of a computer search is a function of the computer's unique features.

R. v. Morelli, [2010] 1 S.C.R. 253 at para. 2

25. First, computers record and store a remarkable amount of information about what users write, see, hear, and do. As noted in *Morelli*, virtually every aspect of one's private life is consolidated into one's computer. They include "our most intimate correspondence", "details of our financial, medical and personal situations", and 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."

R. v. Morelli, *supra* at paras. 3, 105

Kerr, Orin S., "Searches and Seizures in a Digital World", *supra* at 532

Garland, Edward T.M. & Samuel, Donald F., "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?" (2009) 14 Georgia Bar Journal 15 at 16

26. Second, size matters. The computer is no mere container. While computers are physically compact, the amount of data that can be stored on a computer is staggering. For as little as $150, anyone can purchase a computer hard drive with storage capacity of 500 gigabytes, which is roughly equivalent to 250 million pages of text — or about the amount of information contained in all of the books on six floors of an academic library. This is a staggering amount of

data, particularly given that most people do not store academic libraries on their computers, but are more likely to have medical records, personal banking information or intimate journals filling up the same amount of space.

> "Hard Drives" online: PC Mag.com <http://www.pcmag.com/reviews/hard-drives>
>
> Kerr, Orin S., "Searches and Seizures in a Digital World", *supra* at 542

27. Third, computers are notorious for storing a tremendous amount of information that most users do not know about and cannot control. For example, the computer records every Internet site that the computer has visited, sometimes going back years. The Internet cache files store every picture that has come across the computer from the Internet, including those that "pop up" and were not consciously retrieved or saved by the person sitting at the computer. Further, forensic analysts can recover deleted files from a hard drive. Thus, every inappropriate document, photograph, and video that a user ever received from a friend or co-worker likely resides somewhere on her computer even if she deleted it immediately after opening it. In this case, for example, if the Respondent had immediately deleted the impugned images upon finding them, the images would likely still have remained on his computer.

> Garland, Edward T.M. & Samuel, Donald F., "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?", *supra* at 16
>
> Kerr, Orin S., "Searches and Seizures in a Digital World", *supra* at 542
>
> *R. v. Little*, *supra* at para. 96 (S.C.J.)

2. The Information At Issue Is at the "Core" of Informational Privacy

28. The Crown has mischaracterized this appeal as "*Morelli* meets *Gomboc*." (Appellant's Factum, para. 33) While the Crown is correct in acknowledging the applicability of *Morelli*, its attempt to analogize this case to *Gomboc* misses the mark. The Crown's analogy to *Gomboc* undervalues the unique and intimate nature of information stored on a laptop computer.

29. Not all informational privacy is entitled to the same degree of protection. This Court has identified a "core" of informational privacy that will be subject to heightened protection:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect 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. (emphasis added)

R. v. Tessling, *supra* at para. 27

R. v. Plant, [1993] 3 S.C.R. 281 at para. 20

30. The information at issue in *Gomboc* was at the low end of intimacy on the informational privacy spectrum. *Gomboc* involved a s. 8 challenge to the police use of data obtained from the utility company's digital recording ammeter ("DRA"), which recorded patterns of electricity use in the home. The plurality of this Court held that there was no reasonable expectation of privacy in such information because the information recorded by the DRA readings "reaveal[ed] nothing about the intimate or core personal activities of the occupants. It reveal[ed] nothing but one particular piece of information: the consumption of electricity." Such information is remote from the "biographical core of personal information which individuals in a free and democratic society wish to maintain and control from dissemination to the state."

R. v. Gomboc, [2010] 3 S.C.R. 211 at paras. 2, 4

31. In contrast to *Gomboc*, the information at issue in this appeal, as in *Morelli*, is at the "biographical core" of informational privacy. The Respondent was given a computer by his employer, which the employer knew could be used for personal purposes. Not surprisingly, the Respondent stored, among other things, sensitive financial documents on his laptop as well as highly personal photographs of his wife. Such intimate information is a far cry from the household patterns of electricity use that were at issue in *Gomboc*.

R. v. Morelli, *supra* at paras. 2-3, 105

R. v. Gomboc, *supra* at para. 4

Court of Appeal Judgment, A.R., Vol. I, p. 83, para. 86

3. Section 8 Protects Privacy Not Property

32. The fact that the School Board owned the laptop hardware is of limited relevance in this case. The Crown argues that the determinative factor in the reasonable expectation of privacy analysis is the "employer's explicit assertion of ownership over the equipment, network server and data" in the computer (Appellant's Factum, para. 6). This one-dimensional property-based approach to privacy is antithetical to the "large and liberal" interpretation that this Court has

given s. 8 of the *Charter*. The notion that privacy rights are limited by property rights has been roundly rejected since the *Charter*'s inception. As Justice La Forest observed in *Dyment*, "*Hunter v. Southam Inc.* ruptured the shackles that confined [privacy] claims to property." In *Hunter v. Southam*, decided nearly three decades ago, Justice Dickson (as he then was) explained:

> There is, further, nothing in the language of [s. 8] to restrict it to the protection of property or to associate it with the law of trespass. It guarantees a broad and general right to be secure from unreasonable search and seizure.
>
> ...
>
> Construing [the Fourth Amendment] in *Katz v. United States* ... Stewart J. delivering the majority opinion of the United States Supreme Court declared at p. 351 that "the Fourth Amendment protects people, not places". Justice Stewart rejected any necessary connection between that Amendment and the notion of trespass. With respect, I believe this approach is equally appropriate in construing the protections in s. 8 of the Charter of Rights and Freedoms.

Hunter v. Southam, supra at 158

R. v. Dyment, [1988] 2 S.C.R. 417 at 428-429

33. Section 8 of the *Charter* protects privacy, not property. Much of the Crown's submissions proceed on a misunderstanding of this fundamental constitutional principle.

4. Employees Do Not Check Their Privacy at the Workplace Door

34. The fact that this case involves a *workplace* computer does not detract from the force or reasoning of *Morelli*. The distinction between the "work" and "home" computer is a false dichotomy. Employers in this era demand that employees stay connected to the workplace around-the-clock. As such, employer-provided devices (*e.g.*, smart phones, laptops) are ubiquitous. So too is the use of personal computers and phones for work purposes. With the need to remain constantly connected, most people run both personal and work e-mails through the same device. The result is that "work" computers are inevitably used for personal purposes just as "home" computers are inevitably used for work purposes. There is no on/off button between "work" and "personal."

Surowiecki, James, "BlackBerry Season" *New Yorker* (13 February 2012), online: NewYorker.com <http://www.newyorker.com/talk/financial/2012/02/13/120213ta_talk_surowiecki>

35. This is simply a continuation of the trend that Justice Blackmun remarked upon 25 years ago in his dissenting opinion in *Ortega*:

> It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work. ... Consequently, an employee's private life must intersect with the workplace, for example, when the employee takes advantage of work or lunch breaks to make personal telephone calls, to attend to personal business, or to receive personal visitors in the office. As a result, the tidy distinctions (to which the plurality alludes, ...) between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality.
>
> *O'Connor v. Ortega*, 480 U.S. 709 (1987) at p. 15 (Lexis)

36. The reality of the modern workplace is that private, personal tasks must sometimes be completed at work. Those activities are entitled to a reasonable expectation of privacy. If one uses company stationery to write an intimate note to one's spouse on company time, the company is not entitled to the information contained in that note. If one telephones one's doctor from a company telephone, those communications do not belong to the company. Canada's privacy legislation (*e.g., Personal Information Protection and Electronic Documents Act* (*PIPEDA*)) provides robust privacy protections to employees in the workplace vis-à-vis their employers. Further, Canadian courts have generally held that employees enjoy a reasonable expectation of privacy in the workplace vis-à-vis the State. Indeed, the majority of Canadian trial courts to have addressed the specific issue of workplace computers have found that employees do indeed have an expectation of privacy in their workplace computers.

> *PIPEDA*, S.C. 2000, c. 5
>
> Geist, Michael A., "Computer E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance" (2003), 82 Can. Bar Rev. 151 at 168
>
> *R. v. Little*, *supra* at paras. 125, 129, 139 (S.C.J.)
>
> *France (Republic of) v. Tfaily* (2009), 98 O.R. (3d) 161 at para. 29 (C.A.)
>
> *Contra: R. v. Ritter*, [2006] A.J. No. 791 at paras. 30-41 (Prov. Ct.)

37. New technological trends will only exacerbate this phenomenon. The advent of "cloud" or Internet-based computing, for example, makes it possible to access one's data from anywhere on any device. Cloud or Internet-based e-mail services, such as Hotmail and Gmail, have been popular for more than a decade. Now, as companies, government and educational institutions

move data and document management off of their internal networks and onto the Internet and remote networks, cloud computing means that an ever-increasing amount of personal data, documents, videos, photographs, and recordings will be stored and copied in cyberspace — to be accessed and copied onto myriad devices, some of which will be "home" devices and some of which will be "work" devices.

> Barnhill, David S., "Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless" (2010) 25 Berkley Tech. L.J. 621
>
> Acello, Richard, "Get Your Head in the Cloud" *ABA Journal* (1 April 2010) online: <http://www.abajournal.com/magazine/article/get_your_head_in_the_cloud/>
>
> Richmond, Shane, "Apple iCloud: Will the cloud finally go mainstream?" *Telegraph* (28 January 2012) online: Telegraph.co.uk <http://www.telegraph.co.uk/technology/apple/9045477/Apple-iCloud-will-the-cloud-finally-go-mainstream.html>
>
> Eskin, Blake, "iCloud, You Cloud, We All Cloud," *New Yorker* (7 June 2011), online: NewYorker.com <http://www.newyorker.com/online/blogs/newsdesk/2011/06/icloud.html>
>
> Millan, Luis, "Cloud computing on the rise" *Lawyers Weekly* (29 April 2011) online: LawyersWeekly.ca <http://www.lawyersweekly.ca/index.php?section=article&articleid=1402>

38. Accordingly, the Crown cannot be correct that the level of privacy available to individuals under s. 8 of the *Charter* turns solely on the primitive distinction between a "home" and "work" computer. It should be the *nature* of information — not the "work" vs. "home" label — that drives the analysis.

5. Workplace Policies, Modified by Custom and Practice, Permitted Personal Use

39. The Crown relies heavily on the policies governing the use of the Respondent's workplace laptop in this case. But these policies, properly considered, do not weigh against the Respondent's reasonable expectation of privacy in the contents of the laptop. Three questions must be asked: (i) what were the applicable policies? (ii) were the policies consistent with, or modified by, actual practice? (iii) what weight should be given to workplace policies in general? The cumulative effect of the answers to these questions suggests a minimal, if non-existent, role for the factor of workplace policies in this case.

40. First, as Justice Karakatsanis observed in the court below, "there was no clear privacy policy relating to teachers' laptops."

Court of Appeal Judgment, A.R., Vol. I, p. 61, para. 39

41. At the School Board level, the Policy and Procedures Manual (the "Manual") stipulated that "all data and messages generated on or handled by board equipment are considered to be the property" (emphasis added) of the School Board. But as submitted above, the s. 8 inquiry is concerned with privacy, not property. The only explicit restriction on privacy in the Manual concerns email, which the Manual recognized as "private" but which could be opened by administrative staff in certain defined circumstances. On the other side of the ledger, the Manual implicitly endorsed privacy by permitting teachers to engage in "Incidental personal use" of their laptops so long as it does not "consume more than a trivial amount of resources", "interfere with staff productivity", and "preempt any business activity."[2] Indeed, the principal, Bruce Bourget, acknowledged on cross-examination that there was no prohibition on teachers keeping sensitive personal medical information on their laptops.

Court of Appeal Judgment, A.R., Vol. I, p. 61, para. 39

Evidence of Bruce Bourget, A.R., Vol. II, p. 79:12-79:15

Exhibit A – Policy and Procedures Manual, A.R., Vol. II, pp. 174-175

42. At the school level, the only policy that implicated computer privacy was the AUP, which was drafted for students. The parties disagreed, and the trial judge made no finding, on the applicability of the AUP to teachers. On the one hand, the principal testified that he orally advised teachers that the AUP applies to both students and teachers. On the other hand, the AUP applies only to students by its terms; the AUP was signed only by students; and the AUP's terms do not readily translate into a privacy policy for teachers. For instance, the AUP provides: "Teachers and administrators may monitor all student work and e-mail including material saved on laptop hard drivers. Users should NOT assume that files stored on network servers or hard

[2] The Crown's attempt to distinguish between "personal" and "private" use should be rejected (Appellant's Factum, para. 61). Unlike the privacy-property distinction, the dichotomy between personal and private use is not one that has been recognized under s. 8 of the *Charter*. To the contrary, s. 8 exists to protect, among other things, that "biographical core of *personal* information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (emphasis added): *R. v. Gomboc, supra* at para. 2. In addition, the Crown's reliance on the Manual's prohibition on "Inappropriate content" should also be rejected (Appellant's Factum, para. 51). The fact that the technician in this case, and ultimately the police, discovered evidence of a nude student cannot be used to justify the search *ex post facto*. As this Court stated in *R. v. Wong, supra* at 49-50 more than 20 years ago, "the question whether persons who were the object of an electronic search had a reasonable expectation of privacy cannot be made to depend on whether or not those persons were engaged in illegal activities." See also *R. v. A.M.*, [2008] 1 S.C.R. 569 at para. 72.

drives of individual computers will be private." As Justice Karakatsanis observed, this language not only fails to address teacher privacy, but it would also, if applied to teachers, be inconsistent with the Manual's provisions on the very same subject. The Manual states that all teacher emails are "considered private".

Court of Appeal Judgment, A.R., Vol. I, p. 61, para. 40

Exhibit B – Acceptable Use Agreement, A.R., Vol. II, p. 179

43. This confusing patchwork of rules is a far cry from the clarity and breadth of the workplace policies present in many of the U.S. cases relied on by the Crown. For instance, in *U.S. v. Simons,* the employer had a policy that stated: "users shall … understand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate" (emphasis added).[3] This is both clearer and broader than the combined effect of the Manual and the AUP in this case. The narrow and equivocal language of the Manual and the AUP bear more resemblance to the subscriber agreement in *U.S. v. Warchak* (*i.e.,* "NuVox *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service"), in which the Court held that the language was insufficiently broad to "snuff out a reasonable expectation of privacy".[4]

U.S. v. Simons, 206 F.3d 392 (2000) at p. 3 (Lexis)

U.S. v. Warchak, 631 F.3d 266 (2010) at p. 25 (Lexis)

44. Second, to the extent that there were applicable workplace policies that restricted the privacy rights of teachers in this case, they were offset by the actual practices at the school. As

---

[3] See also *U.S. v. Angevine,* 281 F.3d 1130 (2002) at p. 4 (Lexis), in which the workplace policy stated: "The University reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically…to audit the use of University resources." Similarly, in *U.S. v. Busby,* 2011 U.S. Dist. LEXIS 145217 at p. 5 (Lexis), the workplace policy provided: "*Users have no explicit or implicit expectation of privacy.* NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent." And in *U.S. v. Thorn,* 375 F.3d 679 (2004) at p. 4 (Lexis), the workplace policy stipulated: "Employees do not have any personal privacy rights regarding their use of DSS information systems and technology. An employee's use of DSS information systems and technology indicates that the employee understands and consents to DSS'[s] right to inspect and audit all such use as described in this policy."

[4] See also *U.S. v. Long,* 64 M.J. 57 (2006) at p. 13 (Lexis): "Based on our review of precedent and the totality of the circumstances in this case, we conclude that while the log-on banner may have qualified Appellee's expectation of privacy in her e-mail, it did not extinguish it. Simply put, in light of all the facts and circumstances in this case, the "monitoring" function detailed in the log-on banner did not indicate to Appellee that she had no reasonable expectation of privacy in her e-mail."

Justice Karakatsanis held, "the evidence shows that" the policies "were modified…by convention and usage of the teachers' laptops".

Court of Appeal Judgment, A.R., Vol. I, p. 62, para. 41

45. A consideration of workplace policies necessarily includes a consideration of workplace customs and practice. As the plurality of the U.S. Supreme Court held in *O'Connor v. Ortega* — which is the original authority for the workplace policies test relied on by the Crown — the "operational realities" of the workplace include both official office "procedures" and "actual office practices."[5] This is consistent with the totality of the circumstances test in Canadian law under *Edwards/Tessling,* in which the "historical use of the property or item" is considered. It is also consistent with the well-established principle in Canadian employment law that extrinsic evidence of past practice is relevant to the interpretation of an ambiguous contractual term.

O'Connor v. Ortega, supra at pp. 6-7 (Lexis)

R. v. Edwards, supra at para. 45

R. v. Tessling, supra at para. 32

Marianhill Inc. v. Canadian Union of Public Employees, Local 2764, [2009] O.J. No. 2703 at paras. 21-26 (C.A.)

46. The customs and practices at the Respondent's school *support* a reasonable expectation of privacy in the contents of his laptop. As the trial judge found, "Whatever the official policy might have been…the actual policy seems to have been to accept that staff would load private material onto their computers." This finding was based on, among other things, evidence that: (i) the Respondent was given exclusive use of the laptop; (ii) teachers were allowed to use their laptops for limited personal purposes and to take them home during the summer recess; (iii) the Respondent's laptop contained personal financial and tax information and photographs of his wife; and (iv) other teachers stored sensitive personal information on their laptops such as bank account numbers and personal financial data.[6] The trial judge's finding was supported by the

---

[5] See *U.S. v. Long, supra* and *Quon v. Arch Wireless,* 529 F.3d 892 (2008) (Lexis), rev'd on other grounds in *Ontario v. Quon,* 130 S. Ct. 2619 (2010) (Lexis) for examples of U.S. cases in which the actual office practices were held to modify official workplace policies.

[6] The Crown takes issue with the finding that teachers stored sensitive personal information on their laptops such as bank account numbers and personal financial data because neither the Respondent nor any other teachers testified on the *Charter* motion (Appellant's Factum, para. 62). The finding is based, however, on the signed statement of Daryl Smith (*i.e.,* Mr. Taggart's supervisor and a teacher and Program Leader for Technical Student and Laptop Learning), which was prepared at the request of principal, Bruce Bourget. This statement was entered into the record as an

evidence and is entitled to deference. Notably, the Crown does not submit that the trial judge made any palpable and overriding error.

Charter Ruling, A.R., Vol. I, pp. 21-22

Court of Appeal Judgment, A.R., Vol. I, pp. 61-64, paras. 38-45

Exhibit E – Copy of letter dated June 27, 2006 from Daryl Smith to Bruce Bourget, A.R., Vol. II, p. 220

Exhibit "A" to the Affidavit of Michael Venturi sworn November 2, 2007, A.R., Vol. I, p. 107

Evidence of Bruce Bourget, A.R., Vol. II, p. 39:7-39:19

Evidence of Timothy Burtt, A.R., Vol. II, pp. 130:16-130:26, 158:13-158:28

47. Third, and in any event, this Court should be careful not to place too much reliance on workplace policies (or the "operational realities" of the workplace) in the s. 8 analysis. As discussed above, this consideration is rooted in the plurality opinion of the U.S. Supreme Court in *Ortega*. This Court has always been cautious about importing U.S. doctrines into Canadian constitutional law in a piecemeal fashion given the fundamental differences between the two constitutions. It should be especially cautious in this instance because the authoritativeness of the plurality opinion in *Ortega* is questionable even south of the border. Only four members of the Court signed on to the opinion. When the Court was given the opportunity to solidify its correctness in the 2010 case of *Ontario v. Quon,* it declined. In dissent, Justice Scalia continued to criticize the test and lamented the majority's agnosticism and the resulting uncertainty that he predicted it would produce.

Reference re Motor Vehicle Act (British Columbia) S 94(2), [1985] 2 S.C.R. 486 at 498

R. v. Sinclair, [2010] 2 S.C.R. 310 at para. 38

Ontario v. Quon, supra at pp. 12-13 (Lexis)

48. The "operational realities" test has also been widely criticized by the academy in the U.S. Operational realities are, for all practical purposes, unilaterally determined by the employer. Thus, to say that operational realities can be the driving factor in undermining the reasonableness of an expectation of privacy is to permit the employer to violate privacy simply by providing notice. Such an approach has the potential to extinguish privacy rights in the workplace.

Hess, Michelle, "What's Left of the Fourth Amendment in the Workplace: Is the Standard of Reasonable Suspicion Sufficiently Protecting Your Rights?" (2006) 15 Fed. Circuit B.J. 255 at 276, 278

---

exhibit at trial without any objection from Crown counsel. See Evidence of Bruce Bourget, A.R., Vol. II, p. 49:14-49:30. The Crown should not now be permitted to re-litigate this issue.

Conforti, Justin, "Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the *Ortega* Test in *Quon v. Arch Wireless*" (2009) 5 Seton Hall Circuit Rev. 461 at 464, 477

Bayens, Stephan K., "The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology" (2000) 48 Drake L. Rev. 239 at 247

49. This also provides another basis upon which to distinguish this appeal from *Gomboc.* In *Gomboc,* both the plurality opinion of Justice Deschamps and the concurring opinion of Justice Abella relied to some extent on the *Code of Conduct Regulation* in evaluating the reasonableness of the expectation of privacy. The *Regulation* was held to be important because it governed the relationship between the parties. Both Justices Deschamps and Abella, however, were careful to premise the importance of this factor on the ability of the customer to request that his electricity use information be kept confidential from the police. In Justice Abella's words, "The fact that the customer can request that his or her information be protected means essentially that under this *Regulation,* the customer is presented with the unrestricted ability to control the expectation of privacy in his or her relationship with [the utility company]."

R. v. Gomboc, *supra* at paras. 31, 32, 55, 82, 85

50. It cannot be said that the same sort of "unrestricted ability" exists in the workplace where the employer enjoys a significant power advantage. In this context, the terms of the relationship are imposed by one side. An employee (or prospective employee) who does not wish to consent to the employer's monitoring arrangements is unlikely to find herself with a job. Therefore, this Court should be reluctant to rely too heavily on the workplace policies factor in the reasonable expectation of privacy analysis. As Professor Geist has observed, Canadian law has "gradually accepted the premise that surveillance in the workplace…cannot be justified by simple notice" even in the non-*Charter* context. *A fortiori* this should be true under s. 8 of the *Charter.*

Natt Gantt, II, Larry O., "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace" (1995) 8 Harv. J. L. & Tech. 345 at 385, 405-408

Tadros v. Peel Regional Police Service, [2009] O.J. No. 2158 para. 38 (C.A.)

Geist, Michael A., "Computer E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance", *supra* at 178

6. Teachers Do Not Have a Diminished Expectation of Privacy at School

51. The Crown relies on this Court's opinion in *M.R.M.* to argue that teachers have a diminished expectation of privacy at school (Appellant's Factum, paras. 52-56). The application of *M.R.M.* to this case, however, would amount to an unwarranted extension of that case.

R. v. M.R.M., [1998] 3 S.C.R. 393

52. *M.R.M.* concerned a teacher's warrantless search of a student at school. The question in *M.R.M.* was the scope of the student's expectation of privacy at school vis-à-vis their teachers and principals. This Court held that as a result of teachers' unique position as guardians of school safety and the need to respond quickly where students are believed to be carrying dangerous weapons or drugs, students had a lower-than-normal expectation of privacy vis-à-vis their teachers and principals. In so ruling, this Court emphasized that its holding was limited to this specific relationship and context: "This modified standard for reasonable searches should apply to searches of students conducted by teachers within the scope of their responsibility and authority to maintain order, discipline and safety within the school." (emphasis added)

R. v. M.R.M., *supra* at paras. 4-7, 44-51, 55

53. *M.R.M.* did not purport to hold that *teachers* have a diminished expectation of privacy in the school setting. There are sound legal and policy reasons to reject the Crown's invitation to extend *M.R.M.* to teachers.

54. First, teachers are not children. It is inconsistent with an approach to s. 8 that respects teachers' equal human dignity and autonomy to hold that their expectations of privacy can be curtailed in the same manner as schoolchildren.

55. Second, even if *M.R.M.* applied and the teacher's expectation of privacy was diminished vis-à-vis other *school officials*, this diminished expectation does not lead inexorably to a diminished expectation of privacy vis-à-vis *the police*. This Court was careful to draw a distinction between the two types of searches in *M.R.M.* As Justice Cory explained, "a more lenient and flexible approach should be taken to searches conducted by teachers and principals than would apply to searches conducted by the police." This distinction was confirmed in *A.M.* by both Justice LeBel's plurality opinion and Justice Binnie's concurring opinion.

R. v. M.R.M., *supra* at paras. 32, 47

R. v. *A.M., supra* at para. 2 per LeBel J. and paras. 46-47 per Binnie J.

7. The Police Cannot Piggyback on the School Board's Right of Access

56. Finally, to the extent that the Respondent had any diminished reasonable expectation of privacy vis-à-vis his employer, the School Board, the same cannot be said of his reasonable expectation of privacy vis-à-vis the police. There is a long line of cases from this Court that hold that the State cannot "piggyback" on the rights of access of third parties to search or seize items in which the accused has a reasonable expectation of privacy vis-à-vis the State (see paras. 60-69, *infra*.) Thus, Justice Karakatsanis correctly concluded that, "To the extent that the appellant's reasonable expectation of privacy was modified by the technician's implied right of access in relation to maintaining the school's network, this would not extend to a police intrusion to investigate a criminal offence without a warrant."

Court of Appeal Judgment, A.R., Vol. I, p. 74, para. 69

II. THE WARRANTLESS SEARCH WAS UNREASONABLE

57. Once a reasonable expectation of privacy has been recognized, there is a search within the meaning of s. 8 of the *Charter*. The only remaining question is whether the search was reasonable. Warrantless searches are presumptively unreasonable. This presumption can only be rebutted when the Crown carries its burden to show: (i) the search was authorized by law; (ii) the law is reasonable; and (iii) the manner in which the search was carried out is reasonable. The Crown has failed to meet that onus in this case.

R. v. Collins, [1987] 1 S.C.R. 265 at 277-278

A. The Police Cannot Piggyback on the School Board's Right of Access to the Laptop

58. In an attempt to save the warrantless search and seizure of the Respondent's laptop, the Crown argues that the Sudbury Police were entitled to take the laptop from the School Board and examine its contents pursuant to the duty of the principal under the *Education Act* "to maintain proper order and discipline in the school" and "to give assiduous attention to the health and

comfort of the pupils" (Appellant's Factum, para. 86). However, this Court has repeatedly rejected arguments that a state actor can piggyback on the authority of a third party to invade an individual's reasonable expectation of privacy. This is true whether the third party is a private actor or another state actor.

Education Act, R.S.O. 1990, c. E.2, ss. 265(a) and (j)

59. As both the trial judge and the Court of Appeal noted, this case is highly analogous to *Buhay*. In *Buhay,* the Court held that the police could not justify their warrantless search of the accused's belongings from his rented bus depot locker simply because the private security guards who had contacted the police had earlier gone into the same locker with a master key and searched the same belongings. The accused's expectation of privacy was continuous. The intervention of the security guards at the bus depot did not extinguish that privacy interest or "relieve the police from the *Hunter* requirement of prior judicial authorization before seizing contraband uncovered by security guards."

R. v. Buhay, [2003] 1 S.C.R. 631 at paras. 22, 33-34, 38

60. *Buhay* is no outlier in the Court's jurisprudence. In *Dyment*, the Court held that an accused continued to enjoy a reasonable expectation of privacy vis-à-vis the State in a blood sample that had been lawfully obtained by a treating physician. In *Wong,* the Court held that even though the accused invited members of the public to enter his hotel room, he continued to enjoy a reasonable expectation of privacy in the room's activities vis-à-vis the State. (In *Mercer*, the Ontario Court of Appeal, applying *Wong*, excluded evidence of cannabis residue and cash that had been seized from the accused's hotel room despite the fact that the police were permitted to enter the room by hotel staff who had the right to enter the room.) In *Colarusso,* this Court held that the warrantless seizure of the accused's blood and urine samples by the police from the coroner could not be justified by either: (i) the original consent of the accused to provide the samples to the hospital for medical purposes; or (ii) the coroner's statutory authority to seize these samples from the hospital for the purpose of determining whether an inquest was necessary.[7] And in *Evans,* this Court held that while all members of the public have an "implied

[7] The distinction that the Crown draws at para. 91 of its factum between the police actively seeking out a piece of evidence and the police passively receiving it from another entity (private or governmental) is one that this Court has explicitly rejected: see *R. v. Colarusso, supra* at 53.

licence to knock" on another's front door for the purpose of communicating with the occupant of the home, the "implied licence" does not extend to permit the police to approach the front door to gather evidence against the occupant pursuant to a criminal investigation.

R. v. Dyment, *supra* at 430-436

R. v. Wong, *supra* at 52-55

R. v. Mercer, [1992] O.J. No. 137 at paras. 10-15, 24-36 (C.A.)

R. v. Colarusso, [1994] 1 S.C.R. 20 at 60-61, 63, 66-67

R. v. Evans, [1996] 1 S.C.R. 8 at paras. 14-15

61. These cases are based on a purposive view of s. 8 of the *Charter*. As Justice Karakatsanis put it in the court below, "Police are not relieved from the stringent standard of obtaining judicial authorization to conduct a search or seizure based on reasonable and probable grounds, simply because they are provided with evidence in circumstances where the accused's *Charter* rights were either not engaged or were not infringed in the initial gathering of that evidence". This echoes the words of Justice La Forest in *Colarusso* who decried the practice of law enforcement being "permitted to claim the fruits of the search" conducted by another state agent whose "prerequisites of a search may not be as demanding."

R. v. Colarusso, supra at 64

Court of Appeal Judgment, A.R., Vol. I, p. 78, para. 76

62. In the face of this unbroken line of cases from this Court, the Crown cites the U.S. Supreme Court's decision in *U.S. v. Jacobsen*, which held that where an individual's privacy is first invaded by a private party, it may be subsequently invaded by a government actor without a warrant so long as the latter invasion does not exceed the scope of the former. This holding was premised on the assumption of risk doctrine: when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities; and if that occurs, the Fourth Amendment does not prohibit governmental use of that information.

U.S. v. Jacobsen, 104 S. Ct. 1652 (1984) at pp. 14-15 (Lexis)

63. The assumption of risk doctrine, however, has been rejected in Canada ever since this Court overturned the Ontario Court of Appeal's decision in *Duarte*. As Justice La Forest wrote on behalf of the majority of this Court, "No justification for the arbitrary exercise of state power

can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being." This rejection was subsequently reaffirmed in *Wong*. Thus, the Crown's position would require overturning not only *Buhay, Dyment, Mercer, Colarusso,* and *Evans,* but also *Duarte* and *Wong*. To employ a computer analogy, the Crown is trying to reboot an obsolete doctrine, the Commodore 64 of Canadian constitutional law.

R. v. Duarte, [1990] 1 S.C.R. 30 at 48-49

R. v. Wong, supra at 45

64. The Crown also relies on this Court's decisions in *Jarvis* and *Quebec (Attorney General) v. Laroche,* as well as the Ontario Court of Appeal's judgment in *D'Amour,* which the Crown says stand for the proposition that "a government actor engaged in a regulatory function may disclose information to law enforcement for penal investigation when irregularities are found" (Appellant's Factum, para. 86(ii)). But these cases do not articulate such a broad principle.

R. v. Jarvis, [2002] 3 S.C.R. 757

Quebec (Attorney General) v. Laroche, [2002] 3 S.C.R. 708

R. v. D'Amour, [2002] O.J. No. 3103 (C.A.)

65. *Jarvis* involved the transfer of the appellant's books and records from the audit branch of Revenue Canada to the investigation branch of Revenue Canada. *Laroche* involved the transfer of the appellant's rebuilt vehicle files from an auditor at the SAAQ (*i.e.*, a state agency created to ensure that rebuilt vehicles comply with strict regulations for the purpose of road safety) to the police. And *D'Amour* involved the transfer of the appellant's T4 slips from the municipal welfare department to the police. In each of these cases, the courts concluded that the documents could be transferred from the regulatory agency to the investigators without the latter having to obtain a warrant because there could be no reasonable expectation of privacy in the documents transferred given the highly regulated environment in which they were created and maintained.

R. v. Jarvis, supra at para. 95

Quebec (Attorney General) v. Laroche, supra at paras. 83-84

R. v. D'Amour, supra at paras. 56-65 (C.A.)

66. The same cannot be said in this case. Unlike the appellants in *Jarvis, Laroche,* and *D'Amour,* the Respondent was not subject to high regulation. If the School Board can be said to regulate anyone under the *Education Act*, it is the students and not the teachers. And unlike the documents at issue in *Jarvis, Laroche,* and *D'Amour,* the Respondent's school laptop (and that of other teachers in the school) did not simply contain information of legitimate interest to a state regulator. It contained much more. Personal photos, financial data, and Internet browsing information were all stored on the Respondent's laptop. Computers are *sui generis* with respect to the amount of information they contain and, therefore, cannot be compared to a narrow subset of financial documents.

67. Thus, whether or not the School Board and its employees had a limited authority to go into the computer to achieve the objectives of the *Education Act,* the Respondent could not and should not have reasonably expected the police to have been able to conduct a warrantless search of the same computer for the purposes of a criminal investigation.

B. The School Board Had No Authority to Provide Third Party Consent

68. The Crown also cannot justify the warrantless search in this case by pointing to the Respondent's consent. No such consent, whether implicit or explicit, was ever provided vis-à-vis the police. Therefore, the Crown is left to rely on the doctrine of *third party* consent. The Crown argues that the Respondent's employer was entitled to consent to the police search of the Respondent's laptop simply because it owned the laptop and also had access to the laptop. The Court of Appeal correctly rejected this argument. Two observations are in order.

> Court of Appeal Judgment, A.R., Vol. I, p. 75, para. 70

69. First, neither the Crown counsel at trial nor the police officer who conducted the search sought to justify the search on the basis of third party consent. Thus, there is a significant disconnect between the legal basis now being put forward by the Crown and the search that actually took place. The Crown cannot press the "re-set button" because the first argument failed.

70. Second, it is questionable whether the doctrine of third party consent even exists in Canada. The Crown attempts to characterize the lack of jurisprudential support for its position as an under-development of the law (Appellant's Factum, para. 77). However, the paucity of case

law in this area is not by coincidence. Rather, it reflects an understandable reluctance on the part of the judiciary to give life to a doctrine that has the potential to eviscerate the right to privacy under s. 8 of the *Charter*. Consent connotes a waiver of the constitutional right to be secure against unreasonable search and seizure. It must, therefore, be both voluntary and informed in order to be valid. It is difficult to imagine how this can be given by anyone other than the holder of the right.

R. v. D'Amour, supra at para. 64 (C.A.)

R. v. Wills, [1992] O.J. No. 294 at para. 50 (C.A.)

R. v. Mercer, supra at paras. 18-19 (C.A.)

R. v. J.P.W., [1993] B.C.J. No. 2891 at para. 33 (Youth Ct)

R. v. Field, [1996] N.W.T.J. No. 20 at para. 27 (S.C.)

71. The only Canadian cases that the Crown can cite in which the courts have found valid third party consent — and the Crown can only cite two (*Rai* and *Sahid*) — both involve searches of the rooms of children living with their parents.[8] Even within this narrow factual context, these two cases lie in the minority (see *e.g., J.P.W., T.S., Wells,* and *Sandhu* for the opposite holding). Moreover, the holdings in these two cases are based on the notion that children are not fully independent. As the Court observed in *Rai*: "At 18, the accused is not yet an adult with all the privileges and responsibilities being an adult entails." This rationale is hardly applicable to the search of the Respondent's school laptop.

R. v. Rai, [1998] B.C.J. No. 2187 at para. 39 (S.C.J.)

R. v. Sahid, [2011] O.J. No. 653 at paras. 109-118 (S.C.J.)

Contra: *R. v. J.P.W., supra* at para. 36 (Youth Ct); *R. v. T.S.,* [2009] O.J. No. 3877 at para. 13 (O.C.J.); *R. v. Wells,* [1998] O.J. No. 3371 at para. 23 (Gen. Div.); *R. v. Sandhu,* [2005] O.J. No. 5914 at para. 81 (S.C.J.)

72. Beyond this limited factual context, Canadian courts have been very skeptical of claims of third party consent. In *Mercer,* the Ontario Court of Appeal rejected the argument of third party consent where the hotel manager invited the police into the accused's hotel room. In *Field,* the Court rejected the argument of third party consent where the accused handed an envelope to a

[8] While the Crown also cites *R. v. Drakes,* [2009] O.J. No. 2886 (C.A.); *R. v. Figueroa,* [2002] O.J. No. 3138 (S.C.J.), rev'd on other grounds [2008] O.J. No. 517 (C.A.); and *R. v. D.M.F.,* [1999] A.J. No. 1086 (C.A.); all three of these were cases in which the courts found no reasonable expectation of privacy and, therefore, no search within the meaning of s. 8. The issue of third party consent never had to arise.

messenger to be delivered to someone else and the messenger gave the police permission to open it. In *Brilhante,* the Court rejected the argument of third party consent where the accused's wife gave the police consent to search the matrimonial home while the accused was in custody. In *James,* the Court rejected the argument of third party consent where the accused's wife permitted the police to search the accused's desktop computer in the living room. And in *Barrett,* the Court rejected the argument of third party consent where the accused's common law spouse and parents allowed the police to enter the accused's home and search his bedroom.

R. v. Barrett, [1995] O.J. No. 920 at para. 13 (O.C.J.)

R. v. Mercer, supra at paras. 16-23 (C.A.)

R. v. Field, supra at para. 27 (S.C.)

R. v. Brilhante, [2001] O.J. No. 1987 at paras. 27-29 (S.C.J.)

R. v. James, [2005] O.J. No. 4126 at para. 65 (S.C.J.)

73. These cases collectively recognize that s. 8 of the *Charter* protects privacy, not solitude. Just because an individual permits others to access — or even share in the use — of his space does not mean that that individual has given up his privacy over that space vis-à-vis the State. Consent to one is not consent to all.

O'Connor v. Ortega, supra at p. 11 (Lexis)

74. In the face of this jurisprudence, the Crown again urges this Court to look south of the border. The Crown submits that this Court should follow *U.S. v. Matlock,* in which the U.S. Supreme Court held that third party consent is valid where it is based on "mutual use of the property by persons generally having joint access or control for most purposes". In these circumstances, the U.S. Supreme Court held that it is "reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." (emphasis added)

U.S. v. Matlock, 415 U.S. 164 (1974) at p. 10 (Lexis)

75. This position is inconsistent with the analogous decisions in Canada on third party consent (see para. 74, *supra*). But so too is its premise. As was true with *Jacobsen, Matlock* is based on the assumption of risk doctrine, which this Court has unequivocally rejected in *Duarte*.

The Crown's attempt to revive this doctrine — which never won favour above the provincial appellate level — should be rejected. This is not an appropriate case in which to retrofit obsolete and incompatible foreign law to Canadian hardware.

R. v. Duarte, supra at 48-49, 53-54

R. v. Wong, supra at 45

76. In any event, even if the test in *Matlock* were to be applied to the facts of this case, the Crown would not be able to make out valid third party consent. The test is one of "mutual use", not just "mutual access". While the School Board had access to the Respondent's laptop in this case for the purposes of "facilitating" the school's server and keeping "an eye out for problems", use of the laptop belonged entirely to the Respondent. Thus, this case is much more analogous to the facts in *Mercer* than it is to the cases involving the co-occupancy of a residence. Just as the hotel manager in *Mercer* could not consent to a search of the accused's hotel room despite the hotel staff's right to access the room, the School Board could not consent to a search of the Respondent's laptop despite its right to access the laptop.

U.S. v. Matlock, supra at p. 10 (Lexis)

Charter Ruling, A.R., Vol. I, p. 2

77. The contrary suggestion that mutual access alone can give rise to valid third party consent has frightening implications, especially in the digital age of "cloud computing". Nowadays, individuals regularly use web-based email and online storage systems to interact and communicate in what is known as "the cloud" (*i.e.*, a virtual storage space located off-site). (See para. 37, *supra*.)

78. Cloud computing necessarily requires data to be stored with third parties who may access it for the purposes of maintaining the cloud. If this alone can provide the basis for valid third party consent, then companies like Google and Microsoft would be able to consent to police searches of our most intimate files and correspondence without any constitutional oversight. This cannot be the law in Canada. It would amount to the end of privacy rights in, among other things, the Internet-based e-mail accounts offered by Gmail, Hotmail and Yahoo!.

C. There Were No Exigent Circumstances

79. Before moving on to the reasonableness of the manner of search, it is worth noting that there were no exigent circumstances in this case. As Justice Karakatsanis observed, "Once the police had the laptop in their possession, there was no urgency… and a warrant could easily have been obtained." The officer himself conceded that the material on the computer would not have been compromised had he taken the time to go before a judicial officer to seek prior authorization before examining the compact discs and the laptop.

> Court of Appeal Judgment, A.R., Vol. I, p. 73, para. 67
> Evidence of Timothy Burtt, A.R., Vol. II, p. 159:25-159:29

80. That is all that is at issue in this appeal. The Respondent does not contend that the police can never search a workplace laptop for criminal investigation purposes or that the police could not have done so in this case. Rather, the Respondent merely submits that the Sudbury Police should have done what police officers do every day in conducting criminal investigations: get a warrant first. Their failure to do so violated the Respondent's s. 8 *Charter* rights. This step is important to ensure that limits are put on the police power to search electronic devices, carrying as it does the potential to level modern privacy altogether.

D. The Search Was Executed in an Unreasonable Manner

81. In any event, even if the police had the authority to conduct a warrantless search of the Respondent's school laptop (which is denied), they did not execute their warrantless search in a reasonable manner. Instead, the police search of the Respondent's school laptop was overbroad. This gave rise to an independent violation of s. 8 of the *Charter*.

82. As submitted above, computers are capable of storing a staggering amount of information about our most intimate details (see paras. 25-27, *supra*). As such, the search of a computer involves unique problems for privacy that do not exist in any other context. Our correspondence, calendar, medical and financial records, and Internet browsing histories are all concentrated in one device. Thus, the danger that a police search of a computer for a narrow class of evidence will inadvertently reveal everything about our lives is enormous. So too is the danger that less conscientious state actors will use a legitimate search for certain types of evidence as a pretext for

going on a vast fishing expedition into our most private spheres. Any review of the reasonableness of the execution of a computer search must therefore be rigorous in order to adequately guard against these dangers.

> Garland, Edward T.M. & Samuel, Donald F., "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?", *supra* at 16
>
> Kerr, Orin S., "Searches and Seizures in a Digital World", *supra* at 541-543
>
> *R. v. Morelli, supra* at para. 3

83. This is especially the case with warrantless searches. One of the key advantages of requiring a warrant is that it enables an impartial and neutral decision-maker to spell out the ground rules in advance and thereby control to some extent the degree of intrusiveness of the search. The absence of *ex ante* guidelines demand a more exacting *ex post* review.

> *In re Search of 3817 W. West End.*, 321 F.Supp. 2d 953 at pp. 7-8 (N.D. Ill.) (2004) (Lexis)
>
> *R. v. Polius*, [2009] O.J. No. 3074 at para. 57 (S.C.J.)
>
> *R. v. Cross*, [2007] O.J. No. 5384 at para. 21 (S.C.J.)

84. When the facts of this case are measured against these principles, the unreasonableness of the execution becomes apparent. The search was overbroad in two respects: (i) the mirror imaging of the entirety of the laptop's contents; and (ii) the police seizure and viewing of the disc containing the temporary Internet files that captured the Respondent's Internet browsing history.

> *Charter* Ruling, A.R., Vol. I, pp. 8-11, 19
>
> Evidence of Timothy Burtt, A.R., Vol. II, pp. 119:28-120:16, 122:6-122:12, 131:8-131:10, 134:21-134:31
>
> Court of Appeal Judgment, A.R., Vol. I, p. 74, para. 67; p. 78, para. 77

85. The creation of a mirror image of the entire contents of the Respondent's laptop was extremely intrusive. As Justice Karakatsanis noted, the police captured "every piece of personal information that [the Respondent] may have stored on it, including the photographs of his wife, without a warrant."

> Court of Appeal Judgment, A.R., Vol. I, pp. 78-79, para. 77

86. It may be that, as the Crown submits, the need to preserve the integrity of the evidence on a computer during forensic searches might sometimes require a mirror image to be created (Appellant's Factum, para. 94). But where there is a warrantless search that is *prima facie*

unreasonable, the onus should lie with the Crown to explain the necessity of creating a mirror image of the entire computer in the specific circumstances of the case; and to explain the steps taken by the police to ensure that they viewed only those portions of the computer in which they had reasonable and probable grounds to believe they would find evidence of the crime that they were investigating.

87. In this case, the Crown failed to adduce evidence of either the necessity of imaging the entire computer or the precise steps taken by the police to minimize the intrusiveness of the search. All we have is D.C. Burtt's testimony that he was not looking for the Respondent's family pictures and financial records, but only looking for images of child pornography and improper web browsing related to child pornography. The question, however, is not what D.C. Burtt was looking for, but where and how he was looking. On that there is no evidence.

Evidence of Timothy Burtt, A.R., Vol. II, p. 131:8-131:10

88. The overbreadth of the search was further exacerbated by D.C. Burtt's viewing of the Respondent's entire Internet browsing history. As Justice Fish put it in *Morelli,* our Internet browsing history provides the police with "an electronic roadmap of [our] cybernetic peregrinations". Prior to the innovation of the Internet, we might entertain lurid sexual fantasies; speculate about the private lives of our colleagues; and worry about potential illnesses. But we would keep these thoughts largely to ourselves. They would remain hidden in the recesses of our minds. Now, we can surf the Internet for pornography specific to any number of fetishes; stalk our co-workers and their latest photographs on Facebook; and Google our symptoms in search of online medical advice. All of the thoughts that were once available only to the select few in whom we decided to confide are now accessible to the state through an Internet browsing history search. The ability to conduct such searches must be strictly circumscribed.

R. v. Morelli, supra at para. 3

89. In this case, it is not clear why the police had to review the entirety of the Respondent's temporary Internet files in the execution of their search. D.C. Burtt testified that there had been concerns that the images in the temporary Internet files contained a large amount of pornography and concerns of the age of the individuals in those images. But surely the police could have tailored their search to reveal only the image files in the Respondent's Internet browsing history.

And to the extent that the police were interested in any Internet browsing of websites related to child pornography, surely the police could have supplemented an images search with a targeted keyword search. Indeed, the School Board had the technology to carry out such a search. Mr. Taggart testified that the School Board's software gave it the ability to "scan the network for, for any kind of files or folders or key words." It is difficult to imagine that the cyber-crimes unit of the police would not have similar or better technology.

Evidence of Timothy Burtt, A.R., Vol. II, p. 120:13-120:16

Evidence of Ryan Taggart, A.R., Vol. I, p. 135:17-135:22

R. v. Jones, [2011] O.J. No. 4388 at para. 50 (C.A.)

III. THE LAPTOP AND TEMPORARY INTERNET FILES SHOULD BE DEFINITIVELY EXCLUDED UNDER SECTION 24(2)

90. The trial judge correctly excluded the Respondent's laptop and the CD of temporary Internet files under s. 24(2) of the *Charter* and the Court of Appeal properly upheld this exclusion. As this Court held in *Côté,* where a trial judge has considered the proper factors and has not made any unreasonable finding, his determination is owed considerable deference on appellate review.

R. v. Côté, [2011] 3 S.C.R. 215 at para. 44

91. The only error the Court of Appeal committed was in making its ruling on exclusion of the temporary Internet files subject to revision by the trial judge depending on the importance of that evidence to the Crown's case. This Court should clarify that such provisional rulings materially undermine the remedial purpose of s. 24(2) and have no place under the *Charter*.

Court of Appeal Judgment, A.R., Vol. I, p. 85, para. 92

92. In *Grant,* this Court held that the following three factors should be considered in determining whether evidence should be excluded under s. 24(2): (i) the seriousness of the *Charter*-infringing state conduct (admission may send the message that the justice system condones serious state misconduct); (ii) the impact of the breach on the *Charter*-protected interests of the accused (admission may send the message that individual rights count for little); and (iii) society's interest in the adjudication of the case on its merits. Each of these factors is

rooted in the public interests engaged by s. 24(2) and ought to be viewed in a long-term, forwarded-looking and societal perspective. The cumulative effect of these factors supports exclusion in this case.

R. v. Grant, [2009] 2 S.C.R. 353 at para. 71

A. The *Charter*-Infringing State Conduct was Serious

93. The trial judge examined the *Charter*-infringing state conduct in this case and concluded that it was "egregious". Two findings anchored this conclusion, both of which are entitled to deference. As this Court cautioned in *Côté,* "A trial judge's findings of fact on a *voir dire* concerning the admissibility of evidence must be respected unless they are tainted by clear and determinative error." It is worth noting that the Crown does not attempt to meet the *Côté* test for reversing His Honour's finding.

R. v. Côté, supra at para. 52

94. First, the trial judge found that the police could have obtained a warrant before searching the Respondent's laptop and that nothing was gained by circumventing this process. This made the state misconduct more, rather than less, serious. As the trial judge reasoned, "In approaching the situation, the reasonably informed man or woman, aware of the privacy rights of each citizen and appreciative of such rights, would surely insist on due process, particularly when nothing was to be gained by denying it."

Charter Ruling, A.R., Vol. I, pp. 29-30

95. This is consistent with this Court's most recent pronouncement on the relevance of "discoverability" under s. 24(2). In *Côté,* the Court found that "[t]he fact that the police could have demonstrated to a judicial officer that they had reasonable and probable grounds to believe that an offence had been committed and that there was evidence to be found at the place of the search but did not do so, in the circumstances of this case, significantly aggravated the seriousness of their misconduct." The same is true in this case.[9]

---

[9] While *Côté* was not released until after the trial judge's decision in this case, it draws much of its reasoning from the Court's earlier decision in *Buhay.* The trial judge relied heavily on *Buhay* in his s. 24(2) analysis. In particular,

R. v. Côté, supra at para. 82

96. Discoverability can, of course, cut the other way when the police exhibit good faith and/or have a legitimate reason for not seeking prior judicial authorization for the search. But no such reason existed in this case. There were no exigent circumstances. In fact, D.C. Burtt conceded that the material on the computer would not have been compromised had he taken the time to go before a judicial officer to seek prior authorization before examining the discs and the laptop.

R. v. Côté, supra at para. 71

Evidence of Timothy Burtt, A.R., Vol. II, p. 159:25-159:28

97. Moreover, D.C. Burtt was an experienced cyber-crimes officer who should have known better. This was the trial judge's second critical finding. As the trial judge explained:

> It is somewhat surprising that Detective Constable Burtt, who is experienced in cyber crime, took the chance of by-passing the constitutional route to obtain the evidence by launching into a search and seizure operation without first obtaining a warrant. It is even more surprising that he persisted in this course of action when he sent Richard Cole's laptop computer to the Sault Ste. Marie Police Service forensic laboratory for analysis.

Charter Ruling, A.R., Vol. I, p. 31

98. The Crown argues that D.C. Burtt's mistake was "understandable" because when the laptop was searched in 2006, there was no clear appellate authority on the issue of privacy in a workplace computer. While true, that is not how D.C. Burtt conceived of the issue. The Crown's argument might carry more weight if D.C. Burtt had actually considered the question of whether to get a warrant as one that raised novel legal issues; although even then, a reasonable person would expect the police to err on the side of due process especially in the absence of any urgency. But that is not how D.C. Burtt approached the question. D.C. Burtt did not consider the totality of the circumstances and weigh one factor against another. Instead, he considered a single factor determinative: the fact that the laptop was owned by the School Board and not the Respondent. That was all it took for D.C. Burtt to conclude that he did not have to get a warrant. He then persisted in his warrantless search and seizure of the laptop despite the knowledge that teachers

---

trial judge cited and relied on the following statement at para. 63 of the Court's judgment in *Buhay*: "The failure of the police officers to explore the other investigative techniques that were available to them shows the absence of sincere effort to comply with the *Charter*". See *Charter* Ruling, A.R., Vol. I, p. 26.

often put sensitive personal information on their computers including bank account numbers and other personal financial data.

Evidence of Timothy Burtt, A.R., Vol. II, pp. 128:20-129:5, 130:14-130:26, 140:22-140:28, 155:17-155:30
Charter Ruling, A.R., Vol. I, p. 11

99. This conduct demonstrates ignorance of a long established constitutional principle. Section 8 of the *Charter* protects privacy, not property. It protects people, and not places. This principle dates back nearly three decades to *Hunter v. Southam*. Further, D.C. Burtt and his colleagues in the cyber-crimes unit had many years to digest the implications of *Buhay* and *Mercer,* both established law in Ontario. Ownership (or the lack thereof) is not a green light for a warrantless search.

Hunter v. Southam, supra at 159

100. D.C. Burtt's ignorance of this long established constitutional principle cannot be excused. As this Court explained in *Grant,* "ignorance of *Charter* standards must not be rewarded or encouraged and negligence or wilful blindness cannot be equated with good faith".

R. v. Grant, supra at para. 75

101. Thus, Justice Karaktsanis was correct in concluding that "given long established principles that ownership of property is not determinative, the seriousness of the violation, in these circumstances, weighs in favour of exclusion rather than admission of the evidence." The trial judge put it more bluntly: "To confuse ownership of hardware with privacy in the contents of software is not an error which the Court can either tolerate or ignore."

Court of Appeal Judgment, A.R., Vol. I, p. 82, para. 84
Charter Ruling, A.R., Vol. I, p. 24

B. The Impact on the *Charter*-Protected Interests of the Accused Was Severe

102. The second *Grant* factor also militates in favour of exclusion in this case. When one considers, as the trial judge did, that we live "in an age when information is often more valuable than the hardware it is stored in" and "when personal privacy is so tied up with the internet

communications and computer technology", it becomes clear that that search and seizure of the Respondent's school laptop had a very severe impact on his *Charter*-protected privacy interests.

Charter Ruling, A.R., Vol. I, p. 31

103. As Justice Fish wrote in *Morelli,* "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." To be sure, this case involves the search of a workplace computer. But it was a computer that the Respondent's employer permitted for personal use and one in which the Respondent stored extremely personal information such as photographs of his wife. Thus, the rationale underlying Justice Fish's statement in *Morelli* is applicable. To put it at a higher level of generality, as Justice Karakatsanis did in the court below, "Searching a computer that is used for personal purposes is potentially among the most invasive searches." (emphasis added) The police in this case not only searched through the computer, but they created a mirror image of the entire hard drive "without any limitation in scope or method".

R. v. Morelli, supra at para. 2

Court of Appeal Judgment, A.R., Vol. I, pp. 82-83, paras. 85-86

104. The search was similarly invasive with respect to the CD containing the temporary Internet files. As Justice Karakatsanis noted, a search of one's Internet browsing history "can disclose personal preferences and interests, as well as freedoms of thought and association, which [the Respondent] would have a high expectation would remain private." This echoes this Court's observations in *Morelli,* in which it stated that computers can "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." D.C. Burtt searched through all of this information, again "without any limitation in scope or method". This militates strongly in favour of exclusion.

Court of Appeal Judgment, A.R., Vol. I, p. 84, para. 90

R. v. Morelli, supra at para. 105

C. Society's Interest in the Adjudication on the Merits Would Not Be Significantly Impaired by Exclusion

105. Finally, the Court must consider society's interest in the adjudication of this case on its merits. This entails an examination of the reliability of the evidence, the importance of the evidence to the Crown's case, and the seriousness of the offence.

106. The Respondent does not dispute that the evidence of the laptop and the CD of temporary Internet files are reliable physical evidence. Neither piece of evidence, however, is integral to the prosecution in this case. The Crown has evidence of the actual photographs of the student that were found in the hidden folder of the Respondent's laptop, the admissibility of which the Respondent does not contest at this stage. If indeed the student was underage, then the Crown may be able to prove its case for possession of child pornography without resort to the rest of the files in the Respondent's laptop or his Internet browsing history. The relevance of those items of evidence is speculative; and based on the record in this case, they cannot be said to be anything more than peripheral. Thus, Justice Karakatsanis was correct in concluding that the exclusion of this evidence would not exact too great a toll on the truth-seeking goal of the criminal trial.

Court of Appeal Judgment, A.R., Vol. I, p. 83, para. 87; p. 85, para. 91

107. Possession of child pornography is, of course, a serious offence. But there is a spectrum of seriousness for child pornography. Here, the trial judge characterized this as something that would be "at the bottom end of material of that nature" in terms of its seriousness.

Charter Ruling, A.R., Vol. I, pp. 28-29

108. Moreover, as the trial judge noted, "There was no suggestion that this material had been obtained from a paedophile or from someone engaging in the trade of such material, that there was a commercial or exploitative aspect to its production, that it was extorted from those originally making or possessing it or that the very images contained such depiction of human sexuality as would shock the conscience of the average citizen." Instead, the photographs were taken from the computer of the student's ex-boyfriend. And they depicted someone who may turn out to be 18 years or older "in various poses", some of which were "nude shots" and some of which showed her "partially clothed". The Crown itself does not appear to have viewed this as

an especially serious offence as it elected to prosecute the Respondent summarily. As a result, the offence carries a maximum term of imprisonment of only 18 months and a minimum term of 14 days under s. 163.1(4)*(b)* of the *Criminal Code*.

Charter Ruling, A.R., Vol. I, pp. 28-29
Evidence of Bruce Bourget, A.R., Vol. II, pp. 26:25-27:2, 36:7-36:13, 39:10-39:13
Evidence of Timothy Burtt, A.R., Vol. II, p. 162:7-162:10
Criminal Code, R.S.C. 1985, c. C-46, s. 163.1(4)*(b)*

109. In any event, the seriousness of the offence has the potential to "cut both ways". While the failure to effectively prosecute a serious charge due to excluded evidence may have an immediate impact on how people view the justice system, it is the long-term repute of the justice system that is s. 24(2)'s focus. The public may have a heightened interest in seeing a determination on the merits where the offence charged is serious, but it also has a vital interest in having a justice system that is above reproach, particularly where the penal stakes are high.

R. v. Côté, supra at para. 53
R. v. Grant, supra at para. 84

110. This is a case where the seriousness of the offence cuts in favour of exclusion. The implication of the Crown's submission at para. 99 of its factum is that the seriousness of the offence will favour exclusion where the state misconduct is serious (because of the need for the Court to disassociate itself from such misconduct) and favour admission where the state misconduct is understandable or trivial. This is a sensible approach. But where the Crown's submission fails is in its characterization of the police misconduct in this case as "understandable". As submitted above, police ignorance of the long-established constitutional principle that s. 8 of the *Charter* protects privacy and not property is a mistake that cannot be excused. It is understandable only if one assumes and approves of police indifference to the limits of their authority. That is not acceptable. As this Court eloquently stated in *Morelli:*

> Justice is blind in the sense that it pays no heed to the social status or personal characteristics of the litigants. But justice receives a black eye when it turns a blind eye to unconstitutional searches and seizures as a result of unacceptable police conduct or practices.

R. v. Morelli, supra at para. 110

D. The Court of Appeal Should Not Have Made its Exclusion Ruling Provisional

111. The Court of Appeal correctly excluded the evidence of both the Respondent's laptop and the disc of temporary Internet files in this case. The only error it made was in qualifying its ruling with respect to the latter. The Court of Appeal held that because the potential use of the temporary Internet files at trial was "not clear" on the record, it should be open to the trial judge to re-assess the admissibility of this evidence "if the evidence becomes important to the truth-seeking function as the trial unfolds." A provisional ruling of this nature materially undermines the remedial purpose of s. 24(2) of the *Charter.*

Court of Appeal Judgment, A.R., Vol. I, p. 83, para. 87; p. 85, paras. 91-92

112. The Respondent does not dispute the appropriateness of provisional rulings *per se* under s. 24(2) of the *Charter*. The Court recognized in *Calder* that in "very special circumstances" (*i.e.,* where there has been a material change of circumstances), s. 24(2) rulings may be revisited by the trial judge as the trial unfolds. The provisional ruling in this case, however, is problematic because: (i) it was made to depend on circumstances that were or should have been entirely within the knowledge of the Crown at the time of the *voir dire*; and (ii) it enables the s. 24(2) analysis to be overwhelmed by the single sub-factor of the importance of the evidence to the Crown's case. The combined effect of these two features is to materially undermine the remedial purpose of s. 24(2).

R. v. Calder, [1996] 1 S.C.R. 660 at para. 35

113. First, the Court of Appeal's provisional s. 24(2) ruling was made to depend solely on one sub-factor: whether the exclusion of the temporary Internet files would "gut the prosecution". This question, however, is based on matters that were or should have been entirely within the knowledge of the Crown at the time of the *voir dire*. The Crown should be expected to know its own case at the beginning of trial and to be able to explain to the trial judge how a particular piece of evidence fits into the bigger picture of its prosecution.

114. To be sure, the onus lies on the *Charter* claimant to make the case for exclusion under s. 24(2). But the relevance of a particular piece of evidence to the Crown's case is information that lies within the unique knowledge of the Crown. Therefore, where the Crown is unable to

adequately explain this to the courts, the Crown should not be entitled to rely on the argument that exclusion of the evidence would inappropriately gut its case. Nor should the courts invite the Crown to re-make this argument at a later stage in the proceedings where it has not done so to the satisfaction of the Court at the outset. That is especially so in a case like this. The Crown did not object to the timing of the *voir dire* at the beginning of trial nor advance any submissions at trial about its inability to determine the relevance of the evidence in question.

115. Second, the Court of Appeal's provisional ruling sends a dangerous message to lower courts that a sub-factor of the third *Grant* factor — namely, the importance of the evidence to the Crown's case — will be permitted to overwhelm the s. 24(2) analysis. It sends the message that this sub-factor can act as a trump factor.

116. On the Court of Appeal's own analysis, two out of the three *Grant* factors favoured exclusion in this case. Moreover, on the trial judge's analysis, this was not even a particularly serious version of this offence. In these circumstances, it is difficult to imagine a situation in which the importance of the evidence to the Crown's case could alone reasonably justify admission of evidence obtained in violation of the *Charter* under s. 24(2). Yet that is precisely the result that the Court of Appeal's provisional ruling invites.

Charter Ruling, A.R., Vol. I, pp. 28-29

117. If endorsed, such an approach would undoubtedly breed cynicism about the seriousness with which the courts take the *Charter*. It would tell the state that it does not have to pay the price of a jeopardized prosecution for its violations of the *Charter*. And it would tell Canadians that it will only remedy their *Charter* rights under s. 24(2) when there is no price to pay. This Court should unequivocally reject that approach and reiterate its holding in *R. v. Harrison* that "allowing the seriousness of the offence and the reliability of the evidence to overwhelm the s. 24(2) analysis would…in effect, declare that in the administration of the criminal law the ends justify the means." *Charter* rights "must be construed so as to apply to everyone, even those alleged to have committed the most serious criminal offences."

R. v. Harrison, [2009] 2 S.C.R. 494 at para. 40

R. v. Côté, supra at para. 48

PART IV – COSTS

118. The Respondent respectfully requests that he be awarded costs regardless of the outcome of this appeal. In *Trask*, this Court held that the Court has "a broad discretion" to award costs against the Crown even where the Crown is successful.

R. v. Trask, [1987] 2 S.C.R. 304 at 306

119. While cost awards against the Crown in criminal cases are unusual, this appeal is an example of where costs are appropriate. In *Garcia*, Justice Doherty remarked that even in cases where there is no Crown misconduct, it will be appropriate to impose costs on the Crown where "exceptional circumstances exist such that fairness requires that the individual litigant not carry the financial burden flowing from his or her involvement in the litigation."

R. v. C.A.M., [1996] 1 S.C.R. 500 at para. 97

R. v. Garcia (2005), 194 C.C.C. (3d) 361 at paras. 12-13 (Ont. C.A.) (citing *R. v. Trask*, *supra*)

120. In this case, it is manifestly unfair for the Respondent to bear the costs that have flowed from this litigation. This appeal is an unnecessary step in this prosecution. The resultant delay has meant and will continue to mean that the sword of a criminal prosecution hangs over the Respondent while lawyers and judges debate issues of law that may well be moot to the Respondent's case.

121. This case is now in its sixth year of prosecution.[10] Further, assuming the ordinary time lapse between a hearing and decision in this case, the Crown's appeal to the Supreme Court has lengthened an already lengthy case by approximately 21 months.[11]

Information (undated), A.R., Vol. II, p. 87

Charter Ruling, A.R., Vol. I, p. 3

Superior Court Judgment, A.R., Vol. I, p. 35

---

[10] The Respondent was arrested and charged on June 27, 2006. The trial judge rendered his ruling on May 12, 2008. The Superior Court granted the Crown's appeal on April 28, 2009. The Court of Appeal issued its judgment on March 22, 2011. The Crown then sought and obtained leave to appeal to this Honourable Court. A hearing before this Court was subsequently set down for May 15, 2012.

[11] This calculation is based on a projected decision date in this matter of December 15, 2012, which is based on this Honourable Court's statistics indicating that the average time lapse between a hearing and decision exceeded six months in 2011. *See* Supreme Court of Canada, *Statistics 2001-2011: Average Time Lapses*, *available at* http://www.scc-csc.gc.ca/stat/html/cat5-eng.asp.

Court of Appeal Judgment, A.R., Vol. I, p. 47

122. What distinguishes this case from other Crown appeals where proceedings have lasted many years is that the appeal in this case is unnecessary to achieve the Crown's legitimate goals. Whether the Crown wins or loses in this Court, the Respondent will still face another trial in the Ontario Court of Justice. If the Crown's appeal is granted, the Superior Court ruling will be affirmed and the Crown will return to trial with the benefit of all of the previously excluded evidence. If the Crown appeal is dismissed, and the Court of Appeal's order stands, then the Crown will return to trial with the benefit of the disc containing the photographs of the student, which the Court of Appeal refused to exclude and which the Respondent does not challenge before this Court. In either event, the prosecution will have a case to present at trial.

Court of Appeal Judgment, A.R., Vol. I, p. 83, para. 87; p. 85, para. 92

123. By appealing the Court of Appeal's judgment, the Crown chose to pursue a course of action that has all but guaranteed the lengthiest route to either a conviction or acquittal. Six years after he was first arrested, the Respondent remains in jeopardy and faces an inevitable trial at some distant date in the future. In these circumstances, it is reasonable for the Court to order the Crown pay the Respondent's costs.

PART V – ORDERS SOUGHT

124. The Respondent respectfully requests that the Crown's appeal be dismissed and the Crown be ordered to pay the Respondent's costs.

April 12, 2012

ALL OF WHICH IS RESPECTFULLY SUBMITTED

FRANK ADDARIO / GERALD CHAN / NADER R. HASAN

Counsel for the Respondent,
Richard Cole

PART VI – TABLE OF AUTHORITIES

Authority	Paras.
Acello, Richard, "Get Your Head in the Cloud" *ABA Journal* (1 April 2010) online: <http://www.abajournal.com/magazine/article/get_your_head_in_the_cloud/>	37
Barnhill, David S., "Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless" (2010) 25 Berkley Tech. L.J. 621	37
Bayens, Stephan K., "The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology" (2000) 48 Drake L. Rev. 239	48
Conforti, Justin, "Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the *Ortega* Test in *Quon v. Arch Wireless*" (2009) 5 Seton Hall Circuit Rev. 461	48
Dawe, Jonathan, *et al.*, ""We don't need no stinking badges" – or Search Warrants, or Reasonable Grounds, For That Matter: Reasonable Expectations of Privacy in the 21st Century" (Paper presented to the CLA Fall Conference, 9-10 December 2011) [unpublished]	21
Eskin, Blake, "iCloud, You Cloud, We All Cloud," *New Yorker* (7 June 2011), online: NewYorker.com <http://www.newyorker.com/online/blogs/newsdesk/2011/06/icloud.html>	37
Garland, Edward T.M. & Samuel, Donald F., "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?" (2009) 14 Georgia Bar Journal 15	25, 27, 82
Geist, Michael A., "Computer E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance" (2003), 82 Can. Bar Rev. 151	36, 50
"Hard Drives" online: PC Mag.com <http://www.pcmag.com/reviews/hard-drives>	26
Hess, Michelle, "What's Left of the Fourth Amendment in the Workplace: Is the Standard of Reasonable Suspicion Sufficiently Protecting Your Rights?" (2006) 15 Fed. Circuit B.J. 255	48
Kerr, Orin S., "Searches and Seizures in a Digital World" (2006) 119 Harv. L. Rev. 531	23, 25, 26, 27, 82

PART VII – LIST OF STATUTES/REGULATIONS/RULES

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

ENGLISH	FRENCH
Definition of "child pornography" **163.1** (1) In this section, *"child pornography"* means (*a*) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means, (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; (*b*) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act; (*c*) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or (*d*) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act. Making child pornography (2) Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of (*a*) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or (*b*) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term	Définition de « pornographie juvénile » **163.1** (1) Au présent article, *« pornographie juvénile »* s'entend, selon le cas : *a*) de toute représentation photographique, filmée, vidéo ou autre, réalisée ou non par des moyens mécaniques ou électroniques : (i) soit où figure une personne âgée de moins de dix-huit ans ou présentée comme telle et se livrant ou présentée comme se livrant à une activité sexuelle explicite, (ii) soit dont la caractéristique dominante est la représentation, dans un but sexuel, d'organes sexuels ou de la région anale d'une personne âgée de moins de dix-huit ans; *b*) de tout écrit, de toute représentation ou de tout enregistrement sonore qui préconise ou conseille une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi; *c*) de tout écrit dont la caractéristique dominante est la description, dans un but sexuel, d'une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi; *d*) de tout enregistrement sonore dont la caractéristique dominante est la description, la présentation ou la simulation, dans un but sexuel, d'une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi. *Production de pornographie juvénile* (2) Quiconque produit, imprime ou publie, ou a en sa possession en vue de la publication, de la pornographie juvénile est coupable : *a*) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an; *b*) soit d'une infraction punissable sur déclaration de culpabilité par procédure

of ninety days.	sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatre-vingt-dix jours.
Distribution, etc. of child pornography	*Distribution de pornographie juvénile*
(3) Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of	(3) Quiconque transmet, rend accessible, distribue, vend, importe ou exporte de la pornographie juvénile ou en fait la publicité, ou en a en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité, est coupable :
(*a*) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or	*a*) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an;
(*b*) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of ninety days.	*b*) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatre-vingt-dix jours.
Possession of child pornography	*Possession de pornographie juvénile*
(4) Every person who possesses any child pornography is guilty of	(4) Quiconque a en sa possession de la pornographie juvénile est coupable :
(*a*) an indictable offence and liable to imprisonment for a term not exceeding five years and to a minimum punishment of imprisonment for a term of forty-five days; or	*a*) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans, la peine minimale étant de quarante-cinq jours;
(*b*) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of fourteen days.	*b*) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatorze jours.
Accessing child pornography	*Accès à la pornographie juvénile*
(4.1) Every person who accesses any child pornography is guilty of	(4.1) Quiconque accède à de la pornographie juvénile est coupable :
(*a*) an indictable offence and liable to imprisonment for a term not exceeding five years and to a minimum punishment of imprisonment for a term of forty-five days; or	*a*) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans, la peine minimale étant de quarante-cinq jours;
(*b*) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of fourteen days.	*b*) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatorze jours.

Education Act, R.S.O. 1990, c. E.2

ENGLISH	FRENCH
Duties of principal **265.** (1) It is the duty of a principal of a school, in addition to the principal's duties as a teacher, discipline (a) to maintain proper order and discipline in the school; co-operation (b) to develop co-operation and co-ordination of effort among the members of the staff of the school; register pupils and record attendance (c) to register the pupils and to ensure that the attendance of pupils for every school day is recorded either in the register supplied by the Minister in accordance with the instructions contained therein or in such other manner as is approved by the Minister; pupil records (d) in accordance with this Act, the regulations and the guidelines issued by the Minister, to collect information for inclusion in a record in respect of each pupil enrolled in the school and to establish, maintain, retain, transfer and dispose of the record; timetable (e) to prepare a timetable, to conduct the school according to the timetable and relevant school year calendar, to make the timetable and calendar accessible to pupils, teachers, designated early childhood educators and supervisory officers, to assign classes and subjects to teachers and to assign junior kindergarten or kindergarten classes or extended day program units to designated early childhood educators; examinations and reports (f) to hold, subject to the approval of the appropriate supervisory officer, such examinations as the principal considers necessary for the promotion of pupils or for any other purpose and report as required by the board the progress of the pupil to his or her parent or guardian where the pupil is a minor and otherwise to the pupil; promote pupils (g) subject to revision by the appropriate	Fonctions du directeur **265.** (1) En plus de ses fonctions d'enseignant, le directeur d'école exerce les fonctions suivantes : discipline a) maintenir le bon ordre et la discipline dans l'école; collaboration b) accroître la collaboration et la coordination des efforts entre les membres du personnel de l'école; inscription des élèves et cahier de présence quotidienne c) inscrire les élèves et veiller à ce que leur assiduité pour chaque jour de classe soit inscrite soit dans le cahier de présence fourni par le ministre conformément aux instructions qui y figurent, soit d'une autre façon approuvée par le ministre; dossiers d'élèves d) conformément à la présente loi, aux règlements et aux lignes directrices du ministre, recueillir des renseignements en vue de les verser dans un dossier pour chaque élève inscrit à l'école, et constituer, tenir, conserver et transférer le dossier, ainsi que s'en défaire; emploi du temps e) préparer un emploi du temps, diriger l'école en fonction de cet emploi du temps et du calendrier de l'année scolaire pertinent, permettre aux élèves, aux enseignants, aux éducateurs de la petite enfance désignés et aux agents de supervision d'avoir accès à l'emploi du temps et au calendrier, assigner des classes et des matières aux enseignants et assigner des classes de maternelle ou de jardin d'enfants ou des groupes de programme de jour prolongé aux éducateurs de la petite enfance désignés; examens et bulletins scolaires f) faire subir, sous réserve de l'approbation de l'agent de supervision compétent, les examens qu'il juge nécessaires pour le passage des élèves ou dans un autre but, et communiquer les progrès de l'élève, comme le conseil l'exige, à son père, sa mère ou son tuteur, ou à l'élève lui-même s'il est

supervisory officer, to promote such pupils as the principal considers proper and to issue to each such pupil a statement thereof; textbooks (h) to ensure that all textbooks used by pupils are those approved by the board and, in the case of subject areas for which the Minister approves textbooks, those approved by the Minister; reports (i) to furnish to the Ministry and to the appropriate supervisory officer any information that it may be in the principal's power to give respecting the condition of the school premises, the discipline of the school, the progress of the pupils and any other matter affecting the interests of the school, and to prepare such reports for the board as are required by the board; care of pupils and property (j) to give assiduous attention to the health and comfort of the pupils, to the cleanliness, temperature and ventilation of the school, to the care of all teaching materials and other school property, and to the condition and appearance of the school buildings and grounds; report to M.O.H. (k) to report promptly to the board and to the medical officer of health when the principal has reason to suspect the existence of any communicable disease in the school, and of the unsanitary condition of any part of the school building or the school grounds; persons with communicable diseases (l) to refuse admission to the school of any person who the principal believes is infected with or exposed to communicable diseases requiring an order under section 22 of the *Health Protection and Promotion Act* until furnished with a certificate of a medical officer of health or of a legally qualified medical practitioner approved by the medical officer of health that all danger from exposure to contact with such person has passed; access to school or class (m) subject to an appeal to the board, to refuse to admit to the school or classroom a person whose presence in the school or classroom would in the principal's judgment be detrimental to the physical or mental well-being of the pupils; and visitor's book	majeur; passage des élèves g) sous réserve de révision par l'agent de supervision compétent, voir au passage des élèves comme il le juge opportun et remettre à chacun d'eux une attestation à cet effet; manuels h) s'assurer que les manuels scolaires utilisés par les élèves sont ceux que le conseil a approuvés et, dans le cas de matières pour lesquelles le ministre approuve les manuels scolaires, ceux qui sont approuvés par le ministre; rapports i) fournir au ministère et à l'agent de supervision compétent les renseignements qu'il est en mesure de donner concernant l'état des locaux scolaires, la discipline à l'école, les progrès des élèves et d'autres questions touchant les intérêts de l'école, et préparer des rapports à ce sujet pour le conseil comme ce dernier l'exige; mesures d'hygiène vis-à-vis des élèves et entretien des biens scolaires j) accorder une attention soutenue à la santé et au confort des élèves, à la propreté, à la température et à l'aération de l'école, au maintien en état du matériel d'enseignement et des autres biens scolaires, à l'état et à l'apparence des bâtiments et terrains scolaires; rapport au médecin-hygiéniste k) prévenir immédiatement le conseil et le médecin-hygiéniste lorsqu'il a des raisons de soupçonner la présence d'une maladie transmissible dans l'école, et leur signaler l'état insalubre d'une partie des bâtiments ou des terrains scolaires; personne porteuse de maladie transmissible l) refuser l'admission à l'école de la personne qui, selon lui, est atteinte d'une maladie transmissible requérant un ordre aux termes de l'article 22 de la *Loi sur la protection et la promotion de la santé* ou de la personne qui a été en contact avec une telle maladie, jusqu'à la présentation d'un certificat délivré par un médecin-hygiéniste ou un médecin dûment qualifié qu'il a approuvé, indiquant que le danger de contagion résultant du contact avec cette personne est écarté; accès à l'école ou à la classe

(n) to maintain a visitor's book in the school when so determined by the board.	m) sous réserve d'un appel au conseil, refuser d'admettre dans une classe ou à l'école la personne dont la présence dans cette classe ou à l'école pourrait, à son avis, nuire au bien-être physique ou mental des élèves; registre des visiteurs n) tenir un registre des visiteurs dans l'école si le conseil le prescrit.