S.C.C. Court File No. 34268

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

BETWEEN

HER MAJESTY THE QUEEN

Appellant

and

RICHARD COLE

Respondent

APPELLANT'S FACTUM

Restriction on Publication: By Court Order, information that may identify the persons described as the complainant or a witness may not be published, broadcast, or transmitted in any manner, pursuant to the *Criminal Code*, s. 486.4(1)(2)(3) and (4).

AMY ALYEA and FRANK AU
Ministry of the Attorney General
Crown Law Office – Criminal
720 Bay Street, 10th Floor
Toronto, Ontario M5G 2K1
Tel: (416) 326-4600
Fax: (416) 326-4656
E-mail: amy.alyea@ontario.ca
frank.au@ontario.ca

Counsel for the Appellant

ROBERT E. HOUSTON, Q.C.
Burke-Robertson
70 Gloucester Street
Ottawa, Ontario
K2P 0A2
Tel: (613) 236-9665
Fax: (613) 235-4430
E-mail: rhouston@burkerobertson.com

Ottawa Agent for the Appellant

FRANK ADDARIO and
ANDREW FURGIUELE
Sack Goldblatt Mitchell LLP
20 Dundas Street West, Suite 1100
Toronto, ON M5G 2G8
Tel.: (416) 977-6070
Fax: (416) 591-7333
E-mail: faddario@sgmlaw.com

Counsel for the Respondent

COLLEEN BAUMAN
Sack Goldblatt Mitchell LLP
500 – 30 Metcalfe Street
Ottawa, Ontario K1P 5L4
Tel.: 613-482-2463
Fax: 613-235-3041
E-mail: cbauman@sgmlaw.com

Ottawa Agent for the Respondent

Court File No. 34268

IN THE SUPREME COURT OF CANADA

(ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO)

BETWEEN:

HER MAJESTY THE QUEEN

Appellant

-and-

RICHARD COLE

Respondent

APPELLANT'S FACTUM

[*A publication ban was imposed in this matter pursuant to s. 486.4 of the *Criminal Code*]

Table of Contents

PART I – STATEMENT OF FACTS

(A) OVERVIEW

1. Computers have become an integral part of modern life. Use of a work computer is a necessary component of countless types of employment. While our reliance on computers is no longer novel, novel issues of law continue to arise from their use. In the case at bar, this Honourable Court is asked to consider whether a reasonable expectation of privacy arises in a teacher's use of a school board's laptop. The decision in this matter will provide important guidance to law enforcement, employers, employees and lower courts. Whether a reasonable expectation of privacy exists in a work computer must be informed by all of the relevant contextual factors, including the specific work context and the governing information technology (IT) policies. When these factors are properly considered in the totality of the circumstances in the case at bar, the Respondent did not have a reasonable expectation of privacy in the laptop issued to him by his school. As a result, his s. 8 privacy interests were not engaged.

2. The facts of this case also raise the important question of what police are to do when provided computer evidence by an employer who has discovered evidence of crime. Whether a warrant is required will depend on the totality of the circumstances, not on any presumption involving computers. If an employee has a reasonable expectation of privacy in the work computer, the employer's consent may in some cases be sufficient to waive the employee's privacy interest. Where the employer's consent does not apply, a warrantless search may still be reasonable (*e.g.* pursuant to the lawful authority of the *Education Act*). The warrantless search of the laptop and two CDs in this case was reasonable in all the circumstances.

3. Lastly, even if there was a breach of the Respondent's s. 8 *Charter* rights, the administration of justice is better served by admitting all of the computer evidence, having regard to the good faith of the police who were acting in an undeveloped area of law, the reduced expectation of privacy in a work computer, particularly a school computer, and the public interest in getting at the truth of a serious offence – a teacher's alleged possession of child pornography depicting a fifteen year old female student at his school.

(B) THE EVIDENCE AT ISSUE

4. Graphic sexual images of a female grade ten student were discovered on high school teacher Richard Cole's work issued laptop by a school computer technician assessing system stability concerns on the school network. The technician notified the principal and shortly thereafter the school board provided a police officer with (i) a CD containing a screen shot of the "hidden folder" and copies of the images; (ii) a CD of the temporary internet files; and (iii) the laptop used by the Respondent. After meeting with the school board superintendent and reviewing the governing IT policies, the officer sent the laptop to the technological crime unit of the police service for forensic examination without obtaining a warrant for the computer.

5. The Respondent was charged with possession of child pornography (s. 163.1(4) of the *Criminal Code*) and fraudulently obtaining a computer service in the form of data (s. 342.1 of the *Criminal Code*). It was alleged that the Respondent, a communications technology teacher whose responsibilities included monitoring of the school network, had obtained the images of the female student from the computer hard drive of a male student in the school's laptop learning program without the male student's consent or knowledge.

(C) BRIEF HISTORY OF PROCEEDINGS

6. The Respondent was acquitted at trial. The Honourable Mr. Justice Guay of the Ontario Court of Justice found that the Respondent had a reasonable expectation of privacy in the school issued laptop. The trial judge made no reference to the *R.* v. *Edwards/Tessling* criteria for the determination of a reasonable expectation of privacy and relied to a large extent on an analogy to the storage locker in *R.* v. *Buhay*. The trial judge concluded that the warrantless search by police of the computer evidence infringed s. 8 of the *Charter* and that all of the computer evidence should be excluded pursuant to s. 24(2).

> Ruling on *Charter* Motion, Guay J., Ont. Ct., May 12, 2008, Appellant's Record, Vol. I, pp. 5-33
> *R.* v. *Buhay*, [2003] 1 S.C.R. 631
> *R.* v. *Edwards*, [1996] 1 S.C.R. 128
> *R.* v. *Tessling*, [2004] 3 S.C.R. 432

7. The Crown successfully appealed from the decision of Justice Guay and a new trial was ordered by the Honourable Mr. Justice Kane of the Superior Court of Justice. The summary

conviction appeal judge held that the trial judge had erred in law in finding that the Respondent had a reasonable expectation of privacy in the contents of his employer's laptop hard drive. The summary conviction appeal judge concluded, "The *Charter* analysis in this case cannot be determined without considering the respondent's employment context, his employer's ownership of and issuance to him of a laptop computer, and the rules regarding his use of that computer, including the permissibility of personal use and the user's right of privacy." After a thorough consideration of the totality of the circumstances surrounding the Respondent's privacy interest, Justice Kane concluded that the Respondent did not have an objectively reasonable expectation of privacy in the laptop and network server data and ordered a new trial.

Reasons for Decision, Kane J., Sup. Ct., April 28, 2009, Appellant's Record, Vol. I, pp. 35-46

8. The Court of Appeal for Ontario allowed the Respondent's appeal from the summary conviction appeal decision. In a unanimous decision, the Court of Appeal concluded that the Respondent had a reasonable expectation of privacy in the laptop but that it was a "modified" expectation of privacy in regard to the technician, the principal and the school board. As a result, those officials did not breach his s. 8 *Charter* rights. With regard to the CD of the screenshot and images, the Court found that there was no reasonable expectation of privacy in the images, found through the school system, copied onto a CD and passed along to police. There was therefore no police search or seizure of this evidence within the meaning of s. 8 of the *Charter*. However, with regard to both the CD of temporary internet files and the laptop, the Court held that the warrantless search by police was unreasonable and the evidence should be excluded pursuant to s. 24(2). The matter was remitted back to the Ontario Court of Justice for trial. This Court has granted the Attorney General of Ontario leave to appeal from the decision of the Court of Appeal.

Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I, pp. 48-86; leave granted [2011] S.C.C.A. No. 278

(D) THE FACTS

(i) The Discovery of the Sexually Explicit Images of the Female Student

9. A school computer technician was maintaining the school computer server using a "remote desktop" function which allowed the technician to connect to the school's server and actually see a computer's entire desktop, akin to sitting at the computer itself. The technician's

use of new security software identified a large volume of activity between the laptop used by the Respondent and the server, which was a concern to system integrity. There had previously been concerns about the Respondent allowing uses which could de-stabilize the system and a previous network scan using the word "hack" had once led to the Respondent's "My Documents" folder.

Evidence of R. Taggart, Appellant's Record, Vol. I, p. 127, ll. 15-20; p. 130, l. 25 – p. 134, l. 5; p. 135, ll. 10-26; p. 161, l. 13- p. 163, l. 28

10. When the technician looked at the Respondent's "d-drive" through the server, he observed the "My Documents" folder and another called "New Folder". The latter was a "hidden folder", which can be created by a user or a utility or software. By default, most users are not able to see hidden folders but with the software used by the technician the ability to do so was enabled.

Evidence of R. Taggart, Appellant's Record, Vol. I, p. 134, ll. 10-27; p. 167, ll. 1-2

11. When the technician looked at the folder he saw numerous extremely explicit pictures of a young female student. The images appeared to fall within the parameters of the policy against pornography. He took a screen shot which showed some thumbnail pictures of the images. After he confirmed that the young woman in the images was indeed a grade ten student at the school, he informed the principal. The principal attended the technician's office and was shown the screenshot (with a paper held to cover the nudity) and confirmed that the young female was a student at the school. The technician was told to keep the matter confidential. The principal asked the computer technician to copy the screenshot, with the Respondent's name and the path to the pictures, and the images onto a CD so that the principal could give it to the school board. The principal contacted the school board and was told to meet with the Respondent and retrieve the laptop.

Evidence of R. Taggart, Appellant's Record, Vol. I, p. 135, l. 27- p. 136, l. 14; p. 137, l. 19- p. 138, l. 12; p. 139, l. 14-p. 141, l. 31; p. 148, l. 15 – p. 149, l.1
Evidence of B. Bourget, Appellant's Record, Vol. II, p. 25, l. 21 – p. 33, l. 17; p. 52, l. 28 – p. 53, l. 5

12. When the Respondent arrived at school the next morning, the principal accompanied him to his classroom and advised him that there might be inappropriate material on the laptop. After some thought, the Respondent said, "well, there is inappropriate content on there for sure." The principal said he would be taking the laptop and that the Respondent was being sent home with pay. When the principal asked for a current phone number, the Respondent wrote on a scrap of

paper. The Respondent also wrote down the name of a male student and then scribbled it out, explaining that he had obtained the images from that student's laptop.[1] He said that he had not taught or had any involvement with the female student whose images were involved. The Respondent told the principal that there were pictures of his wife on the computer and that he would appreciate it if they were not accessed. The Respondent did not object to giving the laptop to the principal. The principal asked if there were any passwords needed to access the laptop and the Respondent did not write any down. The principal testified that he recalled the Respondent saying that passwords would not be required to get in. The principal acknowledged that the notes he made right after the meeting did not mention that statement by the Respondent. The principal provided the laptop to the school board superintendent.

Evidence of B. Bourget, Appellant's Record, Vol. II, p. 34, l.3 – p. 37, l. 15; p. 38, ll. 8-12; p. 87, l. 24-p. 92, l. 16

13. The school board contacted police. A school superintendent spoke to a cyber crimes officer that night. Arrangements were made for the officer to attend at the school board the next day. The officer met with the superintendent, who provided him with a copy of the school's "Acceptable Use Policy" (AUP). The superintendent told the officer that the Respondent was responsible for its administration. A school board computer technician provided the officer with the laptop and a CD onto which the board technician had copied the Respondent's temporary internet files (surfing history) from the laptop. The officer was advised that the temporary internet files contained a large amount of pornography and that there were concerns about the age of the individuals in those images. The officer then attended at the school and obtained from the principal the CD of the screenshot and images.

Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 116, l. 16 – p. 122, l. 4; p. 152, ll. 2 - 20

(ii) The Employment Context and Applicable IT Policies

14. At the time the explicit images were discovered, in June 2006, the Respondent had been a communications technology teacher at the high school for at least five years. The school was the first secondary school in the province to have a laptop learning program. The laptop used by the Respondent was the property of the school board. Unlike the students, who purchased and supplied their own laptops for use in the laptop learning program, the school provided the

[1] The male student subsequently provided his laptop to the police on consent. Evidence of Cst. Burtt, Appellant's Record, Vol. II, p. 135, l. 24 – p. 136, l. 13

teachers with laptops. The principal testified that the specific laptop at issue had been purchased by the school in 2005 and provided to the Respondent for use in teaching and monitoring the program. The laptop had a sticker on the back clearly marking it as the property of the school. The school's invoice and receipt for the purchase of that laptop were entered as exhibit on the *Charter* motion. Teachers were allowed to take their work laptops home in the evening, on weekends and on summer holidays and "incidental personal use" was permitted.

> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 4, l. 23- p. 11, l. 8; p. 61, ll. 27-29; p. 77, l. 26 – p. 79, l. 31
> Exhibit C – Copy of Purchase Orders, Appellant's Record, Vol. II, pp. 181-183
> Exhibit A – Policy and Procedures Manual, Appellant's Record, Vol. II, p. 175

15. Importantly, the school computer technician testified that the laptop, software *and the information on it* were all property of the school board. The principal testified that the contents of the computer hard drives are not private. The belief that the data on the laptop also belonged to the school board was based in part upon the governing IT policies at the school (set out in more detail below), namely, the Board "Policy and Procedures Manual", the School "Acceptable Use Policy" (AUP) and the Staff Handbook.

> Evidence of R. Taggart, Appellant's Record, Vol. I, p. 142, ll. 10-16; p. 146, l. 6 – p. 148, l. 14; p. 158, l. 25 – p. 160, l. 10
> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 57, ll. 22-25; p. 107, l. 26 – p. 109, l. 1

16. In addition to being the communications technology teacher, the Respondent had a special role as monitor of the laptop learning program. In this role, he was given special computer rights - "domain admin rights" - like those of the school and board IT technicians. These rights allowed the Respondent to access any and all aspects of the network to monitor student activity for inappropriate use or content. Like the IT technicians, his access rights allowed him to set privileges for other users, scan all network traffic and look into the hard drive of any computer plugged into the network. The Respondent was also a member of the school's Computer Planning Committee, which met 2-3 times a year and involved discussions about the school's AUP and whether revisions to the policy were required.

> Evidence of R. Taggart, Appellant's Record, Vol. I, p. 129, l. 22- p. 130, l. 12; p. 160, ll. 13-19
> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 8, l. 12; p. 14, ll. 6-30; p. 15, l. 30 – p. 16, l. 25; p. 18, l. 13 – p. 19, l. 22; p. 46, l. 6 – p. 47, l. 8

(a) The Board Information Technology "Policy and Procedures Manual"[2]

17. The district school board "Policy & Procedures Manual P. 9.06" on information technology provides that "**all board employees are expected to be familiar with and comply with these policies**".

18. It commences with the following "Policy Statement":

> ACCEPTABLE USE OF INFORMATION TECHNOLOGIES
>
> * DISTRICT SCHOOL BOARD SUPPORTS INFORMATION TECHNOLOGY TOOLS THAT FACILITATE STAFF AND STUDENT ACTIVITIES IN SUPPORT OF EDUCATION, RESEARCH, AND BUSINESS FUNCTIONS. IT IS EXPECTED THAT THESE TOOLS ARE USED IN A MANNER CONSISTENT WITH THE BOARD'S MISSION, POLICIES, AND STANDARDS FOR CONDUCT, AND WITH THE EDUCATION ACT FOR ONTARIO.

19. Under "Operational Procedures", the Board "Policy and Procedures Manual" states:

> Information technology systems ***and all data*** and messages generated on or handled by board equipment ***are considered to be the property of * District School Board, and are not the property of users of the information technology.***
>
> * District School Board information technology generally must be used only for business activities. ***Incidental personal use*** is permissible so long as; i) it does not consume more than a trivial amount of resources, ii) it does not interfere with staff productivity, iii) it does not preempt [sic]any business activity.
>
> * District School Board information technology systems may not be used for private business activities, amusement/entertainment purposes, or charitable endeavours unless expressly approved by the * District School Board Director or Chief Financial Officer.
> ...
>
> ***Privacy – Users are not to delete, alter, reposition, or tamper with files belonging to anyone other than themselves. [emphasis added]***

20. The board policy manual prohibits inappropriate content stating: "Users may not post, access or attempt to access material that is inappropriate for a school or administrative office environment, such as (but not limited to) offensive, sexually explicit, obscene, profane, inflammatory, or degrading materials. (See also Policy and Operational Procedures P. 9.05 – Pornographic material)."

21. In regard to email, the Board policy provides:

---

[2] Exhibit A – Board Policy & Procedures Manual, Appellant's Record, pp. 174-177

> Privacy – Email is considered private and the e-mail system is considered property of the * District School Board. ***However, the administrative team can legally open private e-mail if that action seems necessary for the ongoing "health" of the system or inappropriate use is suspected.*** *In cases where access to a users account for system/trouble-shooting purposes is required, attempts to request the user's permission will be made first.* When a user's account is accessed, the user shall be notified. [***emphasis added***; *emphasis in original*]

(b) The School "Acceptable Use Policy" (AUP)[3]

22. The school at which the Respondent taught also had its own policy document on "Acceptable Use of Computers and Networks". Under "Unacceptable Computer and Network Use" it provides that "[c]omputers which connect to the school network are to be used in a responsible, efficient, ethical and legal manner." Among the listed unacceptable uses are "sending or soliciting sexually oriented messages, images, sounds, music, or video."

23. In the privacy section the AUP states: "Teachers and administrators may monitor all student work and e-mail including material saved on laptop hard drives. ***Users should NOT assume that files stored on network servers or hard drives of individual computers will be private.***"[4] Part of the Respondent's teaching role was to provide the AUP to students and collect a signed copy. He was also responsible for monitoring compliance with the policy along with the school computer technicians.

> Evidence of R. Taggart, Appellant's Record, Vol. I, p. 129, l. 22- p. 130, l. 12
> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 18, ll. 5-8
> Exhibit B – Acceptable Use Policy, Appellant's Record, Vol. II, pp. 179

24. The school principal testified that the statement that "users should NOT assume that files stored on network server or hard drives of individual computers will be private" also applied to teachers. He advised the teachers that this policy applies to them at staff meetings at the start of each year, which the Respondent would have attended.

> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 17, l. 10 – p. 18, l. 11

25. The discipline process outlined in the AUP provides, in part, that the student with his or her laptop will be called from class immediately to see a member of the administration, that "the

---

[3] Exhibit B – Acceptable Use Policy, Appellant's Record, Vol. II, pp. 179-180
[4] Emphasis in bold and italics added. Capitalization as per the original.

laptop will be retained for review by a representative from IT" and that "IT will service the laptop and further evidence will be sent to administration in written form signed by IT".

(c) The Staff Handbook[5]

26. Additionally, the teachers were provided with a Staff Handbook at the start of each school year which referenced the AUP. The 2005-2006 handbook states "Desktop computers and network access for laptop users are provided to students for the purposes [sic] school related research and use." It then states that the school board "offers electronic network access to students and staff and each user must understand that the control of the content of the information available on the Internet occurs to limit or block material considered controversial or offensive."

(iii) The Police Considered Whether A Warrant Was Required

27. After receiving the computer evidence from the school, the officer viewed the CD containing the screenshot and images in a secure private area of the cyber crimes unit. He confirmed that there were images which met the definition of child pornography.[6] The officer understood that the initial images that had raised the concern were viewed upon the server, through a connection to the server, and that it was the laptop used by the Respondent that had caused the images to be on the server. He also viewed the CD of temporary internet files and confirmed that there were a large number of images. He did not access the laptop.

> Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 122, ll. 5-11; p. 126, l. 5 – p. 127, l. 18; p. 134, l. 12 – p. 135, l. 22; p. 136, l. 13 – p. 137, l. 6; p. 138, l. 20- p. 139, l. 15

28. The officer contemplated whether he should obtain a search warrant for the laptop. He testified that he would have applied for a search warrant for a *personal* computer from a residence as there was the potential for several privacy interests. In this instance, he considered whether the Respondent might have a privacy interest in the computer, but concluded "based on the information I collected up until the examination of the computer, including the procedures,

---

[5] Exhibit D – Copy of Staff Handbook – 2005/2006, Appellant's Record, Vol. II, p. 212

[6] Section 163.1(1) of the *Criminal Code* defines child pornography as (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 old.

…" that a warrant was not necessary since the laptop and images and data all belonged to the school board and there was no indication of privileged material.

Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 128, l. 20 – p. 132, l. 2; p. 139, l. 15 – p. 141, l. 4; p. 165, ll. 5 - 13

29. Prior to sending the laptop for forensic analysis without warrant, the officer: (i) was provided with a copy of a letter from a teacher to the principal which stated that teachers may have sensitive personal information such as bank account numbers and personal financial data, along with sensitive information about students, on their computers; (ii) spoke to the Respondent twice without the Respondent making any assertion of privacy or ownership on either occasion; and (iii) met again with the superintendent and reviewed the documentation on policies and procedures, including board policy in regard to data contained and created on laptops.

Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 151, l. 25 – p. 152, l. 20; p. 154, l. 13-p.155, l. 23; p. 156, l. 27 – p. 157, l. 7; p. 167, ll. 6-20

30. The officer testified that any privacy interest regarding images of the Respondent's wife could be respected. The officer explained that while a forensic program takes all of the images to recreate an accurate image of the whole computer, the police do not really look for family pictures or financial records or anything else that might be there. He looks specifically for images of child pornography and illegal activity related to child pornography or any other offence. Business computers or any computers may have some personal items but those are respected because the police are not interested in them. He was asked whether personal material kept on a work computer would create a reasonable expectation of privacy and replied, "[i]t depends on policies and procedures." He testified that for example, at the police service they know that computer use is subject to the employer reviewing the hard drive and internet surfing history. Different businesses have different policies in place.

Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 130, l. 22- p. 131, 17; p. 158, l. 28 – p. 159, l. 10; p. 162, l. 13 – p. 163, l. 6; p. 165, ll. 27

PART II – POINTS IN ISSUE

Issue One: How should the existence of a reasonable expectation of privacy in a work computer be assessed?

Issue Two: Whether the warrantless search and seizure of the computer evidence by the police was reasonable?

Issue Three: Did the Court of Appeal err in excluding the computer evidence?

PART III – BRIEF OF ARGUMENT

Issue One: How should the existence of a reasonable expectation of privacy in a work computer be assessed?

(E) OVERVIEW

31. When a school makes the troubling discovery that a teacher has sexually explicit photographs of a grade ten female student on a school supplied laptop, how should we as a society respond? To borrow the words of Justice Dickson in *Hunter v. Southam*, the question is whether the teacher's "interest in being left alone by government" (in using the laptop) must give way to "the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement." Section 8 of the *Charter* is engaged only when the government interferes with a "reasonable expectation of privacy". How should we assess the teacher's claim of a privacy interest in the laptop? In practical terms, can the school officials examine the laptop? Or give it to the police? What are the police to do once they have it?

Hunter v. Southam, [1984] 2 S.C.R. 145 at pp. 159-160

32. To answer these questions, a reasonable person informed of the values underlying the *Charter* would want to know all of the relevant circumstances. Since it was a school computer, what were the rules governing its use? Did the teacher break those rules? How did the school find out about the photographs? What are the school's obligations to the students? Why might they want to hand the laptop to the police? Why should the police accept it? Having done so, what could the police reasonably do with it? These are important questions, and ones that fit comfortably with this Court's s. 8 jurisprudence. In short, the "totality of the circumstances" must be considered.

(F) "TOTALITY OF THE CIRCUMSTANCES" REMAINS THE ANSWER

(i) *Morelli* Meets *Gomboc*

33. The facts of this case place it at the centre of an important legal intersection between this Court's recognition in *R.* v. *Morelli*, of the strong privacy interest found in *personal computers*

within the home and this Court's recognition, in *R.* v. *Gomboc,* that express terms governing use can be absolutely vital to the question of whether or not there is a reasonable expectation of privacy in the totality of the circumstances. It is submitted that whether there is a reasonable expectation of privacy in a *work computer* may very well turn on the IT policies governing an employee's use.

R. v. *Morelli,* [2010] 1 S.C.R. 253
R. v. *Gomboc*, [2010] 3 S.C.R. 211

34. In *Morelli*, this Court recognized, in relation to the search of a personal computer in a home:

> "…it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet."

R. v. *Morelli, supra* at ¶105

35. In *Gomboc*,[7] this Court recognized the importance of regulatory policies in the assessment of whether there was a reasonable expectation of privacy in the information from a digital recording ammeter installed on an individual's residence by the utility company at the request of police. The ultimate conclusion of seven members of the Court was that there was no reasonable expectation of privacy in the circumstances. For four members of the Court, an important factor was that the accused's interest in electricity use data was not exclusive and the supplier had a legitimate use of its own. The utility company was not an interloper exploiting its access to private information to circumvent the *Charter* at the request of the state, but rather a potential crime victim in a wholly cooperative role. For three members of the court, the assessment of the totality of the circumstances turned on the existence of a regulation that authorized the transfer of the information to the police, which dispelled any objectively reasonable expectation of privacy as a result.

R. v. *Gomboc, supra* at ¶¶ 30-34, 41- 43, 57-58, 82- 85, 95

[7] The Court of Appeal for Ontario did not make any reference to the *Gomboc* decision in its analysis. *Gomboc* was released in November 2010, two days after the hearing of the *Cole* appeal but prior to the release of the decision on March 22, 2011.

36. It is important that the powerful language of this Court in *Morelli,* dealing with the expectation of privacy in *personal computers in the home*, not lead inexorably to a determination that *any* computer gives rise to a reasonable expectation of privacy. The Court of Appeal erred by, in essence, presuming the existence of personal privacy interest in a work computer, and failing to properly consider two key contextual factors: the Respondent's specific work environment and the governing IT policies. A proper consideration of these two factors helps to keep the assessment of whether there is a reasonable expectation of privacy in a work computer focused on the individual asserting the privacy right, as opposed to the technology being used. The burden is upon the individual who invokes his or her privacy right to demonstrate, on a balance of probabilities, that he or she has a reasonable expectation of privacy.

Tessling, supra
Gomboc, supra

(ii) Section 8 Protects People Not Computers

37. The asserted constitutionally protected privacy right is that of *the employee* using the work computer. Broad presumptions based upon the nature of the device at issue should not overwhelm the analysis. It is critical that there be an assessment of the totality of the circumstances, as developed in *Edwards/Tessling/Patrick*, in determining whether the employee has established a reasonable expectation of privacy in his or her use of a work computer.

R. v. *Patrick,* [2009] 1 S.C.R. 579

38. The first step, when an accused argues that his or her s. 8 privacy rights under the *Charter* were breached, is to determine if there is a reasonable expectation of privacy in the evidence or place at issue. Only after a reasonable expectation of privacy is established, on a balance of probabilities by the accused, will the Court consider if there is a breach of s. 8 rights. If there is no reasonable expectation of privacy then a warrant is not required.

R. v. *Edwards, supra* at ¶¶45-46
R. v. *Tessling, supra* at ¶¶25-26, 33
R. v. *Patrick, supra* at ¶¶20, 26-28, 81-82

39. The non-exclusive list of contextual factors established by this Court in *Edwards*, developed in *Tessling* and *Patrick*, for assessing whether a reasonable expectation of privacy exists, includes: (i) presence at the time of the search; (ii) possession or control of the property or

place searched; (iii) ownership of the property or place; (iv) historical use of the property or item; (vi) the ability to regulate access, including the right to admit or exclude others from the place; (vi) the existence of a subjective expectation of privacy; and (vii) the objective reasonableness of the expectation.

40. In *R.* v. *Plant*, Justice Sopinka identified several factors that helped to define the parameters of informational privacy:

> Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allows for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.
>
> *R.* v. *Plant*, [1993] 3 S.C.R. 281 at ¶19

41. Ultimately, the analysis is to remain rooted in the core principles established by this Court in *Hunter* v. *Southam*: "… **an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement**." Informational privacy is based on the notion of the dignity and integrity of the individual and the right of the individual to determine for him or herself when, how, and to what extent information about him or her is communicated to others. Section 8 protection extends to "a biographical core of personal information" and includes "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."

Hunter v. Southam, supra at pp. 159-160
R. v. *Dyment*, [1988] 2 S.C.R. 417 at ¶¶16-22
R. v. *Duarte*, 1990] 1 S.C.R. 30 at ¶25

(iii) A Flexible Approach is Required

42. As aptly stated by Justice Binnie for the Court in *Tessling*, "Privacy is a protean concept, and the difficult issue is where the "reasonableness" line should be drawn." Justice Binnie observed that "[c]oncerns should be addressed as they truly arise." Canadian jurisprudence has thus far been able to accommodate technological advances and concomitant changes in privacy interests by establishing a totality of the circumstances approach to privacy rights. The

evaluation of contextual factors within an existing framework provides the necessary flexibility to address the relatively novel issue of when a reasonable expectation of privacy might arise in a work computer.

> *Tessling, supra* at ¶¶25, 55
> *R.* v. *A.M.*, [2008] 1 S.C.R. 569 at ¶¶39-40
> *R.* v. *Wong*, [1990] 3 S.C.R. 36 at ¶¶12, 19-20

43. The United States Supreme Court has so far avoided consideration of whether a reasonable expectation of privacy exists in employer supplied digital devices. In *Ontario* v. *Quon,* the Court concluded that broad categorical pronouncements were not useful given rapidly developing technology and changing privacy expectations. As a result, the Court chose to avoid that issue. *Quon* raised the issue of Fourth Amendment Rights (which protect the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures") in text messages on a police officer's work issued pager. The U.S. Supreme Court assumed, without deciding, a reasonable expectation of privacy because on the facts of that case the search was reasonable. It was conducted for non-investigatory work-related purposes on reasonable grounds and was reasonable in scope.

> *Ontario* v. *Quon*, 130 S. Ct. 2619 (2010), 2010 U.S. LEXIS 4972

44. In a more recent U.S. Supreme Court decision, *United States v. Jones*, Justice Alito made the following *a propos* observation in regard to the leading American *Katz* test which extended Fourth Amendment protection to a person's reasonable expectation of privacy:

> In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the trade off worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.
>
> *United States v. Jones,* 2012 U.S. LEXIS 1063 [Alito J. at p. 46] (Supreme Court of the United States)

45. In that decision, the United States Supreme Court considered whether the government's attachment of a Global Positioning System (GPS) to a vehicle registered to the accused's wife constituted a search. The Supreme Court found that the physical intrusion onto an "effect" to

obtain information constituted a search. The Court confirmed that ownership is not necessarily determinative of Fourth Amendment issues. As a result Justice Scalia, writing for the plurality, did not find it necessary to address the government position that the accused had no reasonable expectation of privacy in the vehicle, as the issue was resolved by the common law-trespass test. Justices Sotomayor and Alito each provided decisions concurring in the judgment but raising some of the unresolved difficulties faced by the courts in dealing with privacy issues and the permissible scope of government intrusion.

United States v. Jones, supra
Katz v. United States (1967), 389 U.S. 347 (Supreme Court of the United States), 1967 U.S. LEXIS 2
Kyllo v. United States (2001), 533 U.S. 27 at 33, 2001 U.S. LEXIS 4487
Mancusi v. DeForte (1968), 392 U.S. 364 (Supreme Court of the United States), 1968 U.S. LEXIS 3075

46. So far, our courts have steered clear of creating broad absolutes, especially in the difficult area of informational privacy, by incorporating new considerations into the existing framework of our constitutionally protected right "to be secure against unreasonable search or seizure". A broad categorical approach involving computers would be a significant deviation from this Court's approach to informational privacy to date. Nor is there any principled reason why it is necessary, given the flexibility of the current framework. It is submitted that the "totality of the circumstances" approach must continue. However, if the decision of the Court of Appeal is allowed to stand it puts that approach at significant risk.

R. v. Patrick, supra at ¶81
R. v. Gomboc, supra at ¶23
R. v. *Vu*, [2011] B.C.J. No. 2487 (C.A.) at ¶¶59-64
R. v. *Jones*, [2011] O.J. No. 4388 (C.A.) at ¶51

(G) KEY CONTEXTUAL FACTORS – *WORK* COMPUTERS

(i) The Governing Information Technology (IT) Policies

47. A key contextual factor emerges from both this Court's recent decision in *Gomboc* and the American jurisprudence on the assessment of reasonable expectation of privacy in work computers: the importance of the governing employee use policies and practices.

48. Unlike Canada, where there are not many decisions on this issue,[8] the American lower courts have had to grapple with the issue of whether a reasonable expectation of privacy exists in relation to work computers. A consistent theme which emerges from that jurisprudence is the importance of workplace policies of use to the determination of reasonable expectations of privacy.

> *United States v. Ziegler*, 474 F. 3d 1184 (9th Cir. 2007), 2007 U.S. App. LEXIS 1952, writ of certiorari denied: 552 U.S. 1105 (2008)
> *United States v. Simons* (2000), 206 F. 3d 392 at 398 (United States Court of Appeal for the 4th Circuit), 2000 U.S. App. LEXIS 2877
> *Asia Global Crossing* (2005), 322 B.R. 247 (United States Bankruptcy Court for the Southern District of New York), 2005 Bankr. LEXIS 415
> See also: *United States v. Warchak* (2010), 631 F. 3d 266 at 287 (United States of Appeal for the 6th Circuit), 2010 U.S. App. LEXIS 25415

49. Moreover, the courts have consistently found that a policy stating that the employer has a right to monitor will be determinative of the issue and will negate any reasonable expectation of privacy.

> *Muick v. Glenayre Electronics* (2002), 280 F. 3d 741 (United States Court of Appeal for the 7th Circuit), 2002 U.S. App. LEXIS 1782
> *United States v. Angevine* (2002), 281 F. 3d 1130 (United States Court of Appeals for the 10th Circuit), 2002 U.S. App. LEXIS 2746
> *United States v. Greiner* (2007), U.S. App. LEXIS 19122 (United States Court of Appeals for the 9th Circuit)
> *Thygeson v. US Bancorp*, 2004 U.S. Dist. LEXIS 18863 (United States District Court for the District of Oregon)
> *United States v. Busby*, 2011 U.S. Dist. LEXIS 145217 (United States District Court for the Northern District of California)
> *United States v. Hassoun* (2007) U.S. Dist. LEXIS 3404 (United States District Court for the Southern District of Florida)
> *United States v. Thorn* (2004), 375 F.3d 679, 2004 U.S. App. LEXIS 14295 (8th Cir.)
> *United States v. Long* (2006) CAAF LEXIS 1216 (United States Court of Appeals for the Armed Forces), reconsideration denied 2006 CAAF LEXIS 1781

50. Since the Respondent's employer was entitled to restrict the terms and conditions of his use of the laptop, and actually did so through the board and school IT policies, it is submitted that whether the Respondent had a reasonable expectation of privacy must be evaluated in the

---

[8] For example: *R. v. Little*, [2009] O.J. No. 3278 (Sup. Ct.); *R. v. Ritter,* [2006] A.J. No. 791 (Prov. Ct.); *France (Republic) v. Tfaily* (2009), 98 O.R. (3d) 161 (C.A.)

context of those governing policies. As Fraser C.J.A. for the Alberta Court of Appeal acknowledged in *Poliquin v. Devon Canada Corp.*[9]:

> Employers have the right to set the ethical, professional and operational standards for their work places. Doing so not only falls within an employer's management rights, it also constitutes an integral component of corporate good governance. The workplace is not an employee's home; and employees have no reasonable expectation of privacy in their workplace computers, the employer is entitled to restrict the terms and conditions on which that use may be permitted.
>
> *Poliquin v. Devon Canada Corp,* [2009] A.J. No. 626 (C.A.) at ¶45

51. In the Respondent's case, it is difficult to reconcile any reasonable expectation of privacy with the combined effect of: (a) the board policy asserting a proprietary right to all data and messages,[10] (b) the school AUP dispelling any privacy interest,[11] and (c) the clear prohibitions against inappropriate uses.[12]

(ii) The Specific Work Environment

52. An expectation of privacy, if it exists at all, may be significantly reduced in a workplace. Thus, the work context of the use of a computer is an important contextual factor. Even more important, in the case at bar, is the *specific* work environment in which the Respondent's employer allowed him use of the laptop – *as a teacher*.

> *R.* v. *Silveira*, [1995] 2 S.C.R. 297 at ¶117
> *Comité paritaire de l'industrie de la chemise* v. *Potash*, [1994] 2 S.C.R. 406
> *R.* v. *Little, supra at* ¶139
> *Poliquin v. Devon Canada Corp, supra* at ¶45

53. As Justice Cory stated in *R.* v. *M.R.M.*:

---

[9] The Court allowed an employer's application for summary dismissal of an employee's wrongful dismissal action where the employee had used a workplace computer for the exchange of pornographic and racist material by email in express violation of the employer's "Code of Conduct."

[10] "Information technology systems and all data and messages generated on or handled by board equipment are considered to be the property of * District School Board and are not the property of users of the information technology."

[11] "Teachers and administrators may monitor all student work and e-mail including material saved on laptop hard drives. Users should NOT assume that files stored on network servers or hard drives of individual computers will be private."

[12] "Users are not to delete, alter, reposition, or tamper with files belonging to anyone other than themselves"; "Users may not post, access or attempt to access material that is inappropriate for a school or administrative office environment, such as (but not limited to) offensive, sexually explicit, obscene, profane, inflammatory, or degrading materials"; "…, the administrative team can legally open private e-mail if that action seems necessary for the ongoing "health" of the system or inappropriate use is suspected"; Unacceptable uses include "sending or soliciting sexually oriented messages, images, sounds, music, or video."

> Teachers and those in charge of our schools are entrusted with the care and education of our children. It is difficult to imagine a more important trust or duty. To ensure the safety of the students and to provide them with the orderly environment so necessary to encourage learning, reasonable rules of conduct must be in place and enforced at schools.
>
> *R.* v. *M.R.M.*, [1998] S.C.R. No. 83 at ¶1

54. In *R.* v. *M.R.M.*, this Court found a diminished expectation of privacy in schools and recognized the reasonableness of warrantless searches by school officials. It is submitted that the jurisprudence finding a diminished expectation of privacy in the school context, albeit dealing with searches of students, must also shape the expectation of privacy analysis in the case at bar. Not only was any expectation of privacy in the use of the laptop not objectively reasonable in light of the IT policies in place and the work context, it was particularly unreasonable given the school environment in which the Respondent worked.

R. v. *M.R.M, supra* at ¶¶34, 35
R. v. *A.M., supra* at ¶65
R. v. *S.M.Z.*, [1998] 131 C.C.C. (3d) 436 (Man. C.A.)
Education Act, R.S.O. 1990, c. E. 2, s. 265(a) and (j)

55. The Respondent's employer was a school board and thus he worked in an environment controlled by common law and statutory obligations. His supervising principal, pursuant to s. 265 of the *Education Act*, had a statutory duty "to maintain proper order and discipline in the school" and "to give assiduous attention to the health and comfort of the pupils." Moreover, the *Education Act* mandates the return of any school property held by a teacher on demand.

Education Act, R.S.O. 1990, c. E. 2, s. 265(a) and (j); s. 264(1)(j)

56. The Court of Appeal, in the judgment below, considered the school environment in their analysis of the reasonableness of the board's search, but failed to give it proper weight in answering the fundamental question of whether the Respondent had a reasonable expectation of privacy in the laptop. Yet, school employment is a key contextual consideration in applying the *Edwards/Tessling* framework. The school board may have given the Respondent temporary possession of the physical laptop, but even that was subject to the board's ultimate control, since the Respondent was under a statutory obligation to return it upon request. Indeed, the handing over of the laptop to the principal by the Respondent appears to be an acknowledgment of his employer's *right of control over the physical computer*. In this context, the Respondent's statements requesting confidentiality in regard to his wife's photographs should be construed as

the Respondent's further acknowledgment of his employer's *right to the data within the laptop,* and thus his subjective recognition that he was not entitled to any privacy in the laptop or its contents. He was simply asking that his employer exercise some sensitivity in relation to that aspect of their full right of access and control. Thus, if he had any reasonable expectation of privacy in his use of the laptop, it was a seriously diminished expectation.

> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 35, l. 3 – p. 37, l. 11
> *Education Act*, R.S.O. 1990, c. E. 2, s. 264(1)(j)

(H) PRIVACY MUST NOT BE PRESUMED IN A *WORK* COMPUTER

57. The Court of Appeal erred by extending the privacy interest established in *personal home computers* to *work computers*, without due regard to the Respondent's specific employment context and the governing IT policies in place for his use of the school laptop. An examination of the Court's consideration of three of the *Edwards* factors best illustrates this error and highlights the importance of considering contextual factors within a totality of the circumstances. If the key contextual factors relevant to the issue are properly examined in that framework, it becomes clear that the Respondent had no reasonable expectation of privacy in his school laptop.

(i) Possession or Control of the Property Searched – *Computer* Not *Data*

58. When the Court of Appeal commenced consideration of the *Edwards* factors, the Court properly noted that, given the remote nature of an electronic search, the accused's presence was not a significant factor. However, the Court then turned to possession and control and stated:

> In this case, the laptop was owned by the school board and was issued for employment purposes. Furthermore, the server, network **and data** belonged to the school board. **However**, the teachers were granted **exclusive possession** of the laptop, including during weekends and vacations, and were permitted to use the laptop for **personal use**. **[emphasis added]**

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 60 at ¶36

59. The Court's construction of the concept of "exclusive possession" of the laptop is problematic. While the teachers may have had exclusive possession of the physical device, it was clear from the board's IT policy that they had no exclusive possession whatsoever of the data contained on it. Moreover, any use of school laptops by the teachers, whether work related or

personal, was subject to the employer's IT policies. Whatever information, whether business related or personal, the teachers placed on school laptops would never be in their "exclusive" possession or control. In this context, if the governing board and school IT policies are given proper consideration, the decision to place personal materials on the laptop is more correctly construed as a conscious abandonment of any personal privacy interests. It is submitted that the Court of Appeal erroneously interpreted "personal use" as *creating* an expectation of privacy contrary to the governing policies.

(ii) Historical Use of the Item – *Personal* Not *Private*

60. The Court of Appeal also erred in its approach to the historical use of the laptop, stating:

> With respect to the reasonable expectation of privacy, **other teachers also used their computers to store sensitive personal information**, such as banking and financial information. The **conventions and customary use by teachers are consistent with a reasonable expectation of privacy**. [**emphasis added**]
>
> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 61 at ¶38

61. While "conventions and customary use" are a relevant consideration, the fact that teachers were allowed "personal use" does not trump the employer's explicit assertion of ownership over the equipment, network server and **data**. The Court emphasized, "[t]he appellant actually used the laptop for personal use as evidenced by the presence of photographs of his wife." However, in considering the allowed "incidental personal use", the Court incorrectly equates "personal use" with "private use", when "personal use" simply means "non-work use." Importantly, the school board's acceptable use policy applied to both work and "non-work use." An employee may choose to store "sensitive private information" on a work computer, but it does not mean that a reasonable expectation of privacy is therefore well-founded, particularly where, as in this case, the Respondent's choice of "sensitive private information" violated the employer's acceptable use policy. Such an expectation flies in the face of the governing IT policies and practices.

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 61 at ¶37

62. Furthermore, the Court of Appeal's reference to "other teachers" in general terms, and the Court's conclusion that "the conventions and customary use by teachers" were consistent with a reasonable expectation of privacy, are troubling given the factual record of this case.[13] The Court found that "other teachers also used their computers to store sensitive personal information, such as banking and financial information", but neither the Respondent nor any other teachers testified on the *Charter* motion. The principal and school computer technician testified that although incidental personal use was permissible, the board owned the laptops and the information on them. The principal and school computer technician also testified that they personally had no expectation of privacy in their use of the school computers. As a result, the evidence of "conventions and customary use" was not sufficient, given the record in this case, to establish an objectively reasonable expectation of privacy in the computer's contents on the part of the Respondent in the totality of the circumstances.

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 61 at ¶38

63. Additionally, the Court's assertion that "there was no clear privacy policy relating to teachers' laptops" failed to acknowledge that, although there was no *separate* policy *specifically addressing teachers' laptops*, it was clear from both board and school policies that network administrators were entitled, and able, to view all data transmitted on the network and stored on hard drives connected to it. As a result, the fact that the teachers were permitted to place personal information on the laptops, when viewed within the totality of the circumstances provided by the

---

[13] The only evidence of personal use by "other teachers" on the *Charter* motion was a letter filed as an exhibit during the cross-examination of the principal. There was no indication that the letter was being admitted for the truth of its contents. The letter was written to the principal by a teacher, not the Respondent, who was the leader of the laptop learning program. It was written to provide the principal with that teacher's statement as to his interaction with the school computer technician when told of the discovery of the images on the Respondent's laptop. In the letter the teacher stated, "I also shared the fact that I, like many teachers, have sensitive personal information on my laptop such as bank account numbers and personal financial data." That teacher did not testify on the motion.

The principal testified that he could not agree or disagree with the teacher's assertion. When asked if the comments in the letter reflected the policy of the school board, the principal responded that "[t]here are things in there that are not congruent." The principal was asked whether he asked other teachers about their personal use as a result of the letter. He responded, "No. No, I have clarified to make sure that they know that computers are for school use, yes, which I have done prior to the issue."

> Evidence of B. Bourget, Appellant's Record, Vol. II, p. 48, l. 27 – p. 50, l. 30; p. 61, l. 30 – p. 64, l. 28
> Exhibit E – Copy of Letter dated June 27, 2006 from D. Smith to B. Bourget, Appellant's Record, Vol. II, p. 221

factual record in this case, does not trump or diminish the employer's ultimate right to the laptop and any information placed in it.

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 61 at ¶39

(iii) Ability to Regulate Access – *Others* Not *Employer*

64. The Court of Appeal's assessment of the ability to regulate access, including the right to admit or exclude others from the place, again demonstrates a failure to adequately consider important contextual factors like the Respondent's specific work environment and the governing IT policies.

65. The Court observes that the Respondent "had the right to keep the laptop in his possession and he protected access to the computer by a password." It appears that the Court saw the Respondent's use of a password as reflecting his ability to exclude others from his laptop and thus as indicative of an expectation of privacy. However, in the circumstances of this case, use of a password was actually more consistent with the employer's need to limit access to its laptop and data to those under the authority of the board, rather than to allow a teacher to prohibit access by his employer.

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 61 at ¶37

66. The Respondent himself acknowledged, when asked by the principal to provide any passwords associated with the laptop, that passwords were not be needed to get in. Indeed, it was the ability of the board and the school to remotely and fully access the laptop without any password which led to the images of child pornography being found in the first place. Further, it was the Respondent's *own ability* to access the laptop hard drive of the male student and obtain the explicit sexual images which led to his alleged possession of child pornography. Thus, the existence of a password on the laptop clearly gave the Respondent no ability whatsoever to regulate the school board's access to the laptop and its contents.

> Evidence of B. Bourget, Appellant's Record, Vol. II, 37, ll. 9-11; p. 89, l. 13 – p. 92, l. 31

67. As the summary conviction appeal judge held, according to the board policies and the school AUP, "Mr. Cole agreed to his employer's right to monitor his work, email and data stored

on his computer drives and therefore waived his right of privacy to this data. ...The network server and its data storage were never in the possession or password control of Mr. Cole."

> Reasons for Decision, Kane J., Sup. Ct., April 28, 2009, Appellant's Record, Vol. I, p. 43 at ¶33

68. The Court of Appeal's reliance upon the fact that there was "no clear unambiguous policy to monitor, search or police the teacher's use of their laptops" presumes a personal privacy interest in a work computer as it implies that such a policy is required to displace an employee's expectation of privacy. However, there is no need for an additional explicit policy for the monitoring or searching of a teacher's laptop in light of (i) the board policy asserting a proprietary right to all data and messages; (ii) the school AUP dispelling any privacy interest; and (iii) the clear prohibitions against inappropriate use.

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 64 at ¶45

69. When evaluated in the totality of the circumstances, including the work environment (a school), the board, school and staff policies of use, the Respondent's own unique role within the school's system administration and the permissible scope of "incidental personal use", there can be no reasonable expectation of privacy in the Respondent's use of the school laptop. As a result the Respondent's s. 8 rights were never engaged.

(I) CONCLUSION: NO REASONABLE EXPECTATION OF PRIVACY

70. The Respondent had no reasonable expectation of privacy in his use of the school laptop. To summarize, the *Tessling/Patrick* framework should be analysed as follows:

1. What was the nature or subject matter of the evidence gathered by the police?

   The subject matter here is the data on the laptop, owned by and accessible to the school board.

2. Did the Respondent have a direct interest in the data?

   Yes, subject to the governing IT policies and work requirements.

3. Did the Respondent have a *subjective* expectation of privacy in the data?

   The Respondent did not testify on the motion. The principal's evidence established that the Respondent was familiar with the school IT policies (including the warning that

computer files are not private and that inappropriate use is prohibited) since he monitored the network and sat on the school Computer Planning Committee. In these circumstances, one is left to wonder whether the Respondent had a *subjective* expectation of privacy at all.

4. Was the Respondent's Expectation of Privacy *Objectively* Reasonable?

   a. *What was the place where the alleged "search" occurred?*

      The alleged "search" took place when (1) a school computer technician accessed the laptop hard drive through the school network; (2) a board technician retrieved temporary internet files from the laptop itself; and (3) the police examined the laptop at its facility.

   b. *Was the informational content of the "search" in public view?*

      The data on the laptop (which belonged to the school board), while not in public view, was "open" to the school employer and in their plain view.

   c. *Had the informational content been abandoned?*

      By choosing to put personal information on the laptop, knowing that any data would become property of the board, the Respondent arguably abandoned any personal privacy interest in the data on the laptop.

   d. *Was the information already in the hands of a third party and, if so, was it the subject of an obligation of confidentiality?*

      The data on the laptop was available (and in fact belonged) to the school board. Since child pornography is, by definition, illegal to possess, the board would have been complicit in a criminal offence if it did not notify the police upon discovery of child pornography on a school laptop. The Respondent could not have expected the board to keep the laptop from the police when it was found to contain materials that are criminal to possess.

   e. *Was the police technique intrusive in relation to the privacy interest?*

      The police simply received from the school board a laptop it owned, with data on the hard drive that also belonged to the board, and copies of some of the

information contained therein. There was no privacy interest in existence at the time of the police intervention.

f. *Was the use of the evidence gathering technique objectively reasonable?*

The police simply accepted from the school employer two CDs they had created of their own data after discovery of inappropriate use, and the laptop itself. While an image of the entire hard drive had to be taken (to preserve the original evidence), the forensic examination of the laptop was properly focused on child pornography. There was no evidence that the police conducted an invasive search that exceeded the legitimate bounds of a child pornography investigation.

g. *Did the informational content expose any intimate details of the Respondent's lifestyle or information of a biographical nature?*

The applicable IT policies permit only "incidental personal use" on the laptop and deny any user claim to privacy. Personal use does not necessarily equate with private use exposing intimate details or information of a biographical nature. In choosing to engage in personal use of the laptop, the Respondent knowingly exposed any informational content to his employer. The Respondent should not be able to rely upon his own inappropriate uses to ground a privacy claim.

71. A workplace computer is not the teacher's castle. Unlike the master of a castle, the teacher does not set the rules; rather, he or she must follow whatever rules are set by the employer. A work laptop is not even the teacher's hotel room or bus locker (both analogies influenced the Court of Appeal). Customers pay the hotel for the privacy of their room, or the bus depot for the security of a rented locker. By contrast, teachers are paid to do the work of their school, using equipment (including computer devices) that belongs to the school and are funded by the taxpayers. In the performance of their duties, including the use of their computers, teachers are accountable to their school board and the public at large. These considerations are part of the totality of the circumstances that must inform the reasonable expectation of privacy analysis.

72. Here, the "rules" explicitly warn the users that their computer files are not private, stipulate that "all data" on school computers belong to the board and prohibit inappropriate use

of the computers. Those who knew about the rules, like the Respondent, when caught breaking the rules, are not entitled to complain that they reasonably expected their computer contents to be private.

Issue Two: Whether the warrantless search and seizure of the computer evidence *by the police* was reasonable?

(J) THE ISSUE DEFINED

73. The Court of Appeal for Ontario did not find any breach of the Respondent's *Charter* rights by the actions of the school officials. The Appellant agrees with that conclusion. The Court also found that the police viewing of the CD of the screenshot and images was not a search or seizure within the meaning of s. 8. The Appellant agrees with that finding too. As a result, the remaining issue is the reasonableness of the warrantless search of the CD of temporary internet files and the laptop by the police.

74. Since the school board employer in this instance was entitled to provide the laptop and CDs to the police,[14] the question then becomes - **what was constitutionally required of the police when provided with that evidence by the employer**? The answer cannot be that whenever the police are provided with computer evidence they must obtain a warrant. It is submitted this "easy answer" is not a principled response. The s. 8 analysis has never been that, because it is possible to seek a warrant, one must be sought. Nor is there a principled reason why an absolute warrant requirement should apply to computers or digital devices. This would create an entirely new and separate category of s. 8 jurisprudence based on the form of the evidence rather than an analysis of whether a reasonable expectation of privacy exists in the totality of the circumstances.

R. v. Patrick, supra at ¶81
R. v. Gomboc,supra at ¶23
R. v. *Vu*, *supra* at ¶¶59-64
R. v. *Jones*, *supra* at ¶51

75. If there is a reasonable expectation of privacy in the computer evidence, then a search or seizure is only reasonable if authorized by law, the law itself is reasonable and the manner of search is reasonable. However, there may not be a "search or seizure" where the employer

[14] See also the discussion below: "Warrantless Search was Reasonable".

simply gives the computer evidence to the police voluntarily, as the privacy interest is then waived. The question for the officer who receives the computer evidence in this way is the validity of the employer's consent. It is submitted that an employer's consent should be valid: (i) where there is mutual use, joint access or control of the work computer, or (ii) where the employee has assumed the risk that the employer will consent to a search of the work computer. The determination is factually driven and based on the totality of the circumstances, including such factors as IT policies and the specific work environment.

R. v. *Collins*, [1987] 1 S.C.R. 265 at ¶23
R. v. *Caslake*, [1988] 1 S.C.R. 51 at ¶12
R. v. *Wills*, [1992] O.J. No. 337 (C.A.) at ¶¶69-71

76. In other instances, a warrantless search of the computer evidence may be reasonable for reasons apart from the employer's consent. For example, a regulatory agency engaged in its audit function may disclose information to the police where irregularities are discovered. In the case at bar, the warrantless search of the laptop and the CDs was reasonable, as will be set out below.

(K) CONSENT BY THE EMPLOYER

77. Although the law on third party consent is not well developed in Canada, the case at bar provides a unique opportunity for this Court to consider how this common law doctrine might apply to computer evidence an employer provides to the police. Specifically, can an employer's consent provide the lawful authority for a reasonable search of a work computer without warrant? It is submitted that it can. In appropriate circumstances a third party may validly waive a person's privacy interest such that s. 8 concerns are not engaged.

78. Although some Canadian courts have recognized third party waiver of s. 8 interests, it does not appear to have arisen in the context of employer consent. To date, the issue has primarily arisen in the context of searches of the bedrooms of individuals still living with their parents. There has been recognition in Ontario and B.C. (*Sahid* and *Rai, infra*) that although the accused had an expectation of privacy in his or her room, the parents' access or control was such that the parents could waive s. 8 protection over the room. The determination is factually driven and the totality of the circumstances approach established in *Edwards* guides the analysis.

R. v. *Sahid*, [2011], O.J. No. 653 (Sup. Ct.) at ¶¶109-118
R. v. *Rai*, [1998] B.C.J. No. 2187 (S.C.) at ¶¶34-48

Contra: *R. v. J.P.W.*, [1993] B.C.J. No. 2891 (Youth Ct); *R.* v. *T.S.*, [2009] O.J. No. 3877 (Ont. Ct.); *R.* v. *Wells,* [1998] O.J. No. 3371 (Gen. Div.); *R.* v. *James*, [2005] O.J. No. 4126 (Sup.Ct.); *R. v. Sandhu,* [2005] O.J. No. 5914 (Sup. Ct.)
R. v. *DiPalma*, [2008] B.C.J. No. 1690 (C.A.) at ¶¶25-28
R. v. *Taylor*, [1999] Y.J. No. 1 (Terr. Ct.) at ¶¶62-68
R. v. *Mercer*, [1991] O.J. No. 137 (C.A.) at ¶¶16-23
See also: *R.* v. *Drakes*, [2009] O.J. No. 2886 (C.A.) at ¶18; *R. v. Figueroa*, [2002] O.J. No. 3138 (Sup. Ct.), reversed on other grounds [2008] O.J. No. 517 (C.A.); *R.* v. *D.M.F.*, [1999] A.J. No. 1086 (C.A.).

79. In the U.S., the "common authority" doctrine[15] set out by the U.S. Supreme Court in *United States v. Matlock* provides two analytical bases for third party consent. "Consent by right" is founded on mutual use, joint access or control. "Consent by assumption of risk" relates to the privacy expectations of the target of the search as to whether someone else would consent to that search. Both concepts are well suited for adaptation in analysing the validity of an employer's waiver of the privacy interests of an employee in a work computer.

United States v. Matlock, 415 U.S. 164 at 172 (1974) (Supreme Court of the United States), 1974 U.S. LEXIS 8

80. American lower courts have repeatedly held that employers could provide valid consent to law enforcement searches of their employees' work computers without warrant.

United States v. Ziegler, *supra*
United States v. Hart (2009) U.S. Dist. LEXIS 72597 at 38-39, 51 (United States District Court for the Western District of Kentucky)
United States v. Greiner, *supra*
U. S. v. Bassignani (2007) U.S. Dist. LEXIS 65648 at 16, reversed on other grounds (2009) U. S. App. LEXIS 6398 (9th Cir. Cal)
Contra: *State of Florida v. Young* (2008) Fla. App. LEXIS 2468 (Court of Appeal of Florida, First District), review denied and US Supreme Court certiorari denied (2009) U.S. SEXIS 694
See also: Lafave, *Search and Seizure: A Treatise on the Fourth Amendment*, Vol. 4, §8.3, Third Party Consent
See also: *United States* v. *Andrus* (2007) 483 F. 3d 711 at 717 (10th Cir.), rehearing denied by, rehearing, en banc, denied by U.S. v. Andrus 499 F 3d 1162 (2007), cert. to US Supreme Court denied 2008 U.S. LEXIS 3083 (U.S. Marc. 31, 2008)

81. In the context of work computers, there are therefore two means by which an employer could provide valid consent, even if the employee has an expectation of privacy in the work

[15] See also: *Frazier v. Cupp*, 394 U.S. 731 at 740 (1969) (Supreme Court of the United States), 1969 U.S. LEXIS 1870; *Illinois v. Rodriguez*, 497 U.S. 177 (1990) (Supreme Court of the United States), 1990 U.S. LEXIS 3295; *U.S. v. Bass*, 661 F. 3d 1299 (2011) (United States Court of Appeal for the 10th Circuit), 2011 U.S. App. LEXIS 23498; *U.S. v. Hunter*, 663 F. 3d 1136 (2011) (United States Court of Appeals for the 10th Circuit), 2011 U.S. App. LEXIS 22882; *United States* v. *Ryerson*, (2008) 545 F. 3d 483 (7th Cir.), 2008 U.S. App. LEXIS 19756.

computer, such that a further search or seizure by police would not require judicial authorization. One is where the employer has the authority to consent in their own right, and another is where the employee has assumed the risk that the employer might permit a search by law enforcement. Employee IT policies and the specific work environment are contextual factors which are likely relevant to both types of consent. It is submitted that, contrary to the finding of the Court of Appeal, the school board's consent provided the cyber crimes officer with lawful authority for a warrantless search and seizure. As will be discussed more fully below, the school board's consent was valid authority under both streams of analysis given the Respondent's specific work environment and the IT policies in place.

R. v. *Wills*, *supra* at ¶¶69-72
R. v. *Borden*, [1994] 3 S.C.R. 145 at ¶¶34-35, 40-41
R. v. DiPalma, *supra* at ¶25
P.G. Barton, "Consent by Others to Search Your Place" 35 Crim L.Q. 441 at pp. 445-447, 450-452
G. Luther, "Consent Search and Reasonable Expectation of Privacy: Twin Barriers to the Reasonable Protection of Privacy in Canada" (2008) 41 U.B.C. L. Rev 1-29 at ¶22
S. Boucher & K. Landa, *Understanding Section 8: Search, Seizure and the Canadian Constitution* (Toronto: Irwin, 2005) at pp. 227-232

(i) Consent "By Right"

82. The Court of Appeal found, in the judgment below, that the officer was not justified in relying upon the consent of the school board to search the computer. However, the assertion of data ownership in the board IT policies established *mutual use*, *joint access* and *control* over any data that a teacher, student or administrator chose to place on a school IT system. Thus the board was uniquely situated, having given notice of ownership and proprietary rights, to waive the Respondent's s. 8 interest as the owner of not only *the laptop* at issue, but *the data within*. As a result, consent of the school board was sufficient to authorize any further examination of the computer evidence by the police.

Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at p. 75 at ¶70

(ii) Consent By "Assumption of Risk"

83. The school board could also consent to the police search of the Respondent's laptop based on "consent by assumption of risk." This consent relates to the privacy expectations of the target of the search as to whether someone else would consent to a search. One would think that

common sense, and not just the governing IT policies, made it clear to a teacher that if the board discovered, in the course of system maintenance, evidence of child pornography (especially when it related to a student at the school) that any privacy right the teacher might have had in their use of the laptop was subsumed by the board's right to provide the laptop to the police.

84. Additionally, once the school board became a victim of crime as a result of the Respondent's use of their property for the ongoing commission of a criminal offence, the board was entitled to cooperate with the police. If the individual spheres of privacy in the laptop overlapped, the right of the board to open up their sphere of privacy to the police necessarily opened up the Respondent's sphere of privacy. In these circumstances, the consent given by the crime victim for the police to examine the information in question should be an acceptable substitute for the absence of prior judicial authorization.

> *R.* v. *Gomboc, supra* at ¶42
> R. W. Hubbard, P.M. Brauti & S.K. Fenton, *Wiretapping and Other Electronic Surveillance: Law and Procedure* (Aurora: Canada Law Book, 2008) at §2.2.3

85. Applied to the school environment, the words of the Supreme Court of New Hampshire in *State of New Hampshire* v. *Collins* are compelling:

> The employer in this case had an affirmative duty to protect his tenants, which is distinct from and independent of any citizen's general obligation to aide in the detection of crime. The employer's own interest is thus identical with the interest of the government in detecting crime, and in these circumstances, no employee could sensibly understand his employer to have limited his own power to detect crime in his own business by placing business property off-limits to the police, simply because the employee was allowed to make personal use of the property when he was not using it to discharge his assigned business responsibilities.
>
> *State of New Hampshire* v. *Collins*, 133 N.H. 609 at 617 (1990), 1990 N.H. LEXIS 115

(L) WARRANTLESS SEARCH WAS REASONABLE

86. If this Court rejects the above consent analysis, it is submitted that the warrantless search of the computer evidence in this case was still reasonable, for the following reasons:

(i) There was lawful and reasonable authority for the school officials to search the laptop. The initial search was authorized by the governing IT policies and the subsequent actions of school officials were authorized by both those policies and the *Education Act*.

> *Education Act*, *supra* s. 265(a) and (j)

(ii) There was lawful and reasonable authority for the school officials to transfer the laptop and CDs to the police. First, the *Education Act* required the Respondent to deliver the laptop to the school board on demand. Second, it is a common law principle that a government actor engaged in a regulatory function may disclose information to law enforcement for penal investigation when irregularities are found. Third, once the laptop was found to contain child pornography, the board could not have kept it without being complicit in a criminal offence (*i.e.* possession of child pornography).

R. v. Jarvis, [2002] 3 S.C.R. 757 at ¶¶88-90, 93, 95
Quebec (Attorney General) v. Laroche, [2002] 3 S.C.R. 708 at ¶¶83, 84
R. v. D'Amour, [2002] O.J. No. 3103 (C.A.) at ¶¶56-65
Education Act, R.S.O. 1990, c. E. 2, s. 264(1)(j)

(iii) The same lawful and reasonable authority which enabled the board to transfer the laptop and CDs to the police (without a warrant) also enabled the police to examine the transferred items without a warrant.

(iv) The manner of search was reasonable. The forensic examination of the laptop by police was properly focused on child pornography. There was no evidence that the police conducted an invasive search that went beyond the legitimate bounds of a child pornography investigation.

87. The first two points above are not controversial. The Court of Appeal held that the actions of the school officials did not violate the Respondent's s. 8 rights and the Appellant agrees with that conclusion. Therefore, the discussion below will focus on the last two points.

(i) The Police were Entitled to Examine the Laptop and CDs

88. It is well established that a regulatory agency engaged in its audit function may disclose information to the police where irregularities are discovered (if the investigation is for the same purpose as the original collection of information, and the collection preceded the investigation). Therefore, the school officials in this case had lawful authority to transfer the laptop and CDs to the police without a warrant.

R. v. Jarvis, *supra*
Quebec (Attorney General) v. Laroche, *supra*
R. v. D'Amour, *supra*

89. The same lawful authority which enabled the school to transfer the items to the police also enabled the police to examine them without a warrant. For example, in *R.* v. *D'Amour*, the Court of Appeal for Ontario held that welfare authorities could disclose to the police personal financial information collected in the administration of social assistance, and the police could use that information for a criminal investigation of fraud related to receipt of the social assistance benefits. The Court held that a recipient of a benefits program would have a reasonable expectation that information provided to establish eligibility would be verified and, if false, be used to prosecute for fraudulent receipt of benefits. In that case, the police properly examined the accused's T4 slips without obtaining a warrant, even though the T4 slips would normally attract s. 8 protection.

R. v. D'Amour, *supra*

90. In contrast, the Court of Appeal said in the case at bar, "the fact that the discs and laptop in this case had been lawfully seized by the principal and the school board and delivered to the police does not affect the continuing privacy expectations". With respect, it is hard to understand how the Respondent's diminished expectation of privacy in an employer-provided laptop can, upon lawful discovery of a criminal offence by the employer, be converted into a full reasonable expectation of privacy *vis-à-vis* the police. It is also difficult to comprehend why a s. 8 *Charter* breach should be found in relation to the police when the IT policies in place permitted the school board employer to hand over their property, *the equipment and data*, to the police when they discovered that a teacher had images of child pornography of a student on the computer.

Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I, p. 78 at ¶76
Muick v. Glenayre Electronics, supra
R. v. *M.R.M., supra* at ¶¶1 & 36
Education Act, *supra* s. 265(a) and (j), s. 264(1)(j)

91. Unlike the safe in *R.* v. *Law*, relied upon by the Court of Appeal, which had been stolen from the accused who therefore maintained an expectation of privacy, the laptop used by the Respondent was always "open" to his employer, in whose possession and control the data remained. Moreover, the police did not seek the computer evidence – the school board turned it over to them in light of the child pornography they had discovered. Unlike *R.* v. *Colarusso*, this was not a case of the police improperly "piggy-backing" on another state actor's lawful seizure.

Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I, pp. 76-79 at ¶¶74-77
R. v. *Law*, [2002] 1 S.C.R. 227 at ¶¶18, 22
R. v. *Colarusso*, [1994] 1 S.C.R. 20 at ¶¶82, 86

92. The Court of Appeal's conclusion that the police search of the CD with the temporary internet files constituted a s. 8 breach is particularly troubling. The school board made a copy of this information while the laptop was in their possession. As the Court noted, there was "no basis upon which to find that the school board breached s. 8 in its search of the laptop or by copying the temporary internet files for the school board's own use." Why then should a reasonable expectation re-emerge when the board voluntarily turned it over to the police? The board informed the officer that the CD contained numerous pornographic images, which violated the acceptable use policy, and that there was a concern about the age of some of the individuals portrayed, which raised the possibility that the CD contained child pornography. It was entirely reasonable in these circumstances that the officer examined what had already been examined by the Respondent's employer to determine if there was evidence of an offence.

Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I, p. 73 at ¶66, p. 79 at ¶79
Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 120, ll. 13-16

93. Similarly, American courts have found that where a government search does not exceed the scope of search of a private actor, Fourth Amendment concerns do not arise. In the circumstances of the case at bar, where the scope of the search by police did not exceed the scope of the school board employer's authority to search, s. 8 *Charter* concerns do not arise. The school board's ownership of the laptop and the data therein provided sufficient authority for the police to search these items.

United States v. *Jacobsen*, 104 S. Ct. 1652 (1984), 1984 U.S. LEXIS 53
U.S. v. Guindi (2008) 554 F. Supp. 2d 1018 at 1021-1025 (U.S. District Ct. for the Northern District of California), 2008 U.S. Dist. LEXIS 59580
United States v. Starr, (2008) 533 F. 3d 985 at 994 (8th Cir.), cert denied 129 S. Ct. 746 (2008), 2008 U.S. App. LEXIS 13305
See also: *United States* v. *Pierce*, 893 F. 2d 669 at 674 (5th Cir. 1990), 1990 U.S. App. LEXIS 73

(ii) The Manner of Search was Reasonable

94. Finally, the police searched the laptop in a reasonable manner. In relation to the imaging of the entire hard drive, the cyber crimes officer explained that it was done to ensure a proper image. Other courts have recognized that the need to preserve the integrity of the evidence on a computer during forensic searches may require a mirror image to be created. The forensic

examination is then conducted on the mirror image, rather than the original hard drive, which ensures that the process of searching does not overwrite the hard drive and alter the original evidence. Against this background, the Court of Appeal's finding that "the police technique was intrusive in copying the entire contents of the hard drive" appears misplaced.

R. v. *Little, supra* at ¶¶164, 166
R. v. *Jones, supra* at ¶¶ 44, 50
R. v. *Bishop*, [2007] O.J. No. 3806 (Ont. Ct.) at ¶¶42-44

95. Contrary to the Court of Appeal's view, there was nothing in the record to suggest that the forensic examination of the laptop was unduly invasive. The cyber crimes officer testified that a computer search focuses on images or other evidence of child pornography; there was no interest in the Respondent's photos, financial records, *etc.* The Court's criticism implies that it would be sufficient to simply identify and preserve the images of child pornography without examining anything else. However, an image alone may be of limited probative value if the imbedded information contained on the laptop along with the image is not also examined. For instance, the creation date, last accessed date and other metadata may all afford circumstantial evidence necessary to prove beyond a reasonable doubt that the Respondent had possession of the child pornography. Finally, it may not be possible to simply extract from a computer the suspect images or files, as even deleted or moved files may be recovered. In this case, there was simply no evidence of an invasive search that exceeded the proper bounds of a child pornography investigation.

Evidence of Cst. T. Burtt, Appellant's Record, Vol. II, p. 131, ll. 3-18
Evidence of R. Taggart, Appellant's Record, Vol. II, p. 170, ll. 19-28

Issue Three: Did the Court of Appeal Err in Excluding the Computer Evidence?

(M) THE COMPUTER EVIDENCE SHOULD BE ADMITTED

96. If this Court concludes that there was a s. 8 violation, it is submitted that all of the computer evidence should be admitted, based on a proper application of *R. v. Grant*. The repute of the administration of justice is better served by admitting the evidence, having regard to the good faith of the police acting in an undeveloped area of the law, the reduced expectation of privacy in a work computer, and society's interest in getting at the truth of a serious offence.

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

(N) THE DECISION OF THE COURT BELOW

97. The Court of Appeal excluded the CD of the temporary internet files and the laptop. In relation to the search of the laptop by the police, the Court of Appeal found, "there was no reckless disregard or wilful blindness because there was no clear appellate court authority on the issue of privacy in a workplace computer." Nonetheless, citing this Court's decision in *Morelli*, the Court of Appeal concluded that computer searches are "highly intrusive" and therefore the laptop should be excluded. As for the CD containing the temporary internet files, the Court of Appeal said that the potential use of this evidence in the trial was "not clear".[16] In the result, the Court excluded the evidence with a caveat: "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."

> Reasons for Judgment, Court of Appeal, March 22, 2011, Appellant's Record, Vol. I at pp. 82-85 at ¶¶84-88, 92

(O) THE *GRANT* ANALYSIS

98. With respect, the Court of Appeal was wrong to conclude that admitting the computer evidence in this case would bring the administration of justice into disrepute. Applying the revised approach to s. 24(2) set out in *Grant*, the important question is "whether a reasonable person, informed of all relevant circumstances and the values underlying the *Charter*, would conclude that the admission of the evidence would bring the administration of justice into disrepute." The "relevant circumstances" in this case include the following:[17]

> *Grant, supra* at ¶68 [Emphasis added]

(i) Seriousness of the State Conduct

a. This case is one of first impression. In 2006 when the laptop was searched, there was no clear appellate court authority on the issue of privacy in a workplace

[16] The Court noted, at ¶91, "there was some suggestion that this data could be used to rebut an innocent explanation for the possession of the pictures on the appellant's hard drive."

[17] The "relevant circumstances" are analysed below according to the three inquiries identified in *Grant, supra* at ¶71: (1) the seriousness of the *Charter*-infringing state conduct; (2) the impact of the breach on the *Charter*-protected interest of the accused; and (3) society's interest in the adjudication of the case on its merits.

computer. Indeed, the school's laptop learning program was the first of its kind in Ontario.

Evidence of Mr. Bourget, Appellant's Record, Vol. II, p. 7, l. 4

b. If the police erred in not obtaining a warrant, it was an "understandable" error. Three levels of court below have disagreed on whether a reasonable expectation of privacy attached to the laptop in question. If this Court were to find that a warrant was required, the police could be forgiven for coming to a different conclusion.[18]

c. There was no wilful or flagrant disregard of the *Charter*. Unlike *Buhay*, where the officers' "casual attitude" towards the warrant requirement aggravated the breach, in this case, Constable Burtt specifically considered the warrant issue, and relied on information provided by the school to determine that a warrant was not required. Any error made by the officer in this regard was not unreasonable.

R. v. Buhay, *supra* at ¶60
Evidence of Constable Burtt, Appellant's Record, Vol. II, p. 128, l. 20 - p. 132, l. 2

d. Good faith on the part of the police reduces the need for the court to disassociate itself from the police conduct.[19] A reasonable person apprised of the above circumstances would conclude that the *Charter*-infringing state conduct in this case was not serious (*i.e.* "the effect of admitting the evidence would not greatly undermine public confidence in the rule of law").

Grant, supra at ¶¶75, 133

(ii) Impact on the Accused's Charter Interest

e. To the extent there was any expectation of privacy in the workplace computer, school policies governing the use of the computer reduced that privacy interest. The lower expectation of privacy attenuates the seriousness of any intrusion at this stage of the analysis.

Grant, supra at ¶113; *R. v. Belnavis*, [1997] 3 S.C.R. 341 at ¶40

---

[18] The learned summary conviction appeal judge, like the police, concluded that a warrant was not required: Reasons for Decision, Kane J., Sup. Ct., April 28, 2009, Appellant's Record, Vol. I, p. 45 at ¶42

[19] See also *R. v. Smith* (2005), 199 C.C.C. (3d) 404 at ¶61 (B.C.C.A.): "To sum up, good faith connotes an honest and reasonably held belief."

f. Moreover, the police conducted the computer search in a responsible manner. While an image of the entire hard drive had to be taken, the forensic examination was focused on child pornography. As Constable Burtt explained, "I'm not looking for Mr. Cole's family pictures. I'm not looking for Mr. Cole's financial records. I'm not looking for anything that may be in there. What I'm looking for are images of child pornography or improper internet – not internet searches but web browsing where there may be access of child pornography and illegal activity related to child pornography or any other offence."

Evidence of Constable Burtt, Appellant's Record, Vol. II, p. 131, ll. 11-17

g. Any privacy interest the Respondent might have had in the laptop was further diminished in that the police clearly had grounds to obtain a search warrant. The availability of the same evidence through lawful means significantly diminishes the impact of the *Charter* breach, where the police acted in good faith and reasonably believed they were entitled to do what was ultimately held to be unconstitutional.

R. v. Cote, [2011] 3 S.C.R. 215 at ¶72; *R. v. Harris* (2007), 87 O.R. (3d) 214 at ¶70 (C.A.); *R. v. Ramage*, [2010] O.J. No. 2970 at ¶51 (C.A.)

(iii) Society's Interest in Getting at the Truth

h. Both the reliability of the evidence (the laptop was reliable physical evidence that existed independently of any *Charter* violation) and its importance to the Crown's case supported the admission of the evidence. This Court said in *Grant*, "exclusion of relevant and reliable evidence may undermine the truth-seeking function of the justice system and render the trial unfair from the public perspective, thus bringing the administration of justice into disrepute."

Grant, supra at ¶81

i. The forensic examination of the laptop is critical to the prosecution's case. Without this evidence, the Crown cannot establish: (i) what metadata the images of child pornography contain (created, accessed, modified dates); (ii) whether any other computer activity was occurring on the laptop at the time that the images

were saved to that location; and (iii) whether these images were ever viewed, copied, or transmitted on the laptop. A reasonable doubt may well arise from a failure to address these issues.

R. v. Morelli, supra at ¶¶36, 66
R. v. Garbett, [2008] O.J. No. 917 (Ont. Ct.), aff'd [2010] O.J. No. 2000 (Sup. Ct.)

j. As discussed earlier, the Court of Appeal left open the possibility of revisiting the exclusion of the temporary internet files should the evidence become important as the trial unfolds. As a general approach to s. 24(2) this is a welcome development, consistent with the truth-seeking function of a criminal trial and the jurisprudence. Nonetheless, for the reasons given above, it is submitted that the temporary internet files should not have been excluded in the first place.

See *e.g. R. v. Calder*, [1996] 1 S.C.R. 660 at ¶35; *R. v. Laboucan*, [2010] 1 S.C.R. 397 at ¶15

(P) CLARIFYING THE SERIOUSNESS OF THE OFFENCE

99. In *Grant*, the majority held that the seriousness of the offence "may be a valid consideration", but it has the "potential to cut both ways." Indeed, the seriousness of the offence may "cut both ways" in cases where both the alleged offence and the state misconduct are serious, and there are competing public interests in "seeing a determination on the merits" and "having a justice system that is above reproach". But here, those interests are not seriously in conflict. In some cases, like this one, the seriousness of the offence cut one way – in favour of admitting the evidence. Specifically, the police made an "understandable" error in a completely undeveloped area of the law. This is not a case where the court must disassociate itself from the police conduct in order to maintain a "justice system that is above reproach". On the other hand, society's interest in an adjudication on the merits is undeniable. Where a teacher is alleged to have possessed child pornography, including sexually explicit images of an underage student at his school, on a laptop that belonged to the school, the public interest in getting at the truth is self-evident. It is the exclusion of the computer evidence that would bring the administration of justice into disrepute.

Grant, supra at ¶84
R. v. Sharpe, [2001] 1 S.C.R. 45 at ¶¶28, 94, 103

PART IV: SUBMISSION ON COSTS

100. The Appellant notes that the Respondent sought costs on the leave application. It is the Appellant's position that costs should not be awarded on the appeal. The prevailing convention in criminal practice is that an accused is not entitled to costs unless there is a marked and unacceptable departure from the usual and reasonable standards of prosecution. The decision of the Attorney General for Ontario to bring this issue of national importance to this Honourable Court does not give rise to such an exceptional remedy.

PART V: ORDER REQUESTED

101. It is respectfully submitted that the appeal should be allowed and a new trial should proceed with the admission of all the computer evidence.

ALL OF WHICH is respectfully submitted by:

Amy Alyea
Counsel for the Attorney General of Ontario

Frank Au
Counsel for the Attorney General of Ontario

PART VI: AUTHORITIES CITED

Statutes:

PART VII: STATUTORY PROVISION

crime, horror, cruelty and violence, shall be deemed to be obscene.

R.S., 1985, c. C-46, s. 163; 1993, c. 46, s. 1.

de l'un ou plusieurs des sujets suivants, savoir : le crime, l'horreur, la cruauté et la violence.

L.R. (1985), ch. C-46, art. 163; 1993, ch. 46, art. 1.

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.

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.

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 of ninety days.

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 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

(3) Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of trans-

Distribution de pornographie juvénile

(3) Quiconque transmet, rend accessible, distribue, vend, importe ou exporte de la pornographie juvénile ou en fait la publicité, ou en a

mission, making available, distribution, sale, advertising or exportation any child pornography is guilty of

(*a*) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or

(*b*) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of ninety days.

en sa possession en vue de la transmettre, de la rendre accessible, de la distribuer, de la vendre, de l'exporter ou d'en faire la publicité, est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de dix ans, la peine minimale étant de un an;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatre-vingt-dix jours.

Possession of child pornography

(4) Every person who possesses any child pornography is guilty of

(*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

(*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.

(4) Quiconque a en sa possession de la pornographie juvénile est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans, la peine minimale étant de quarante-cinq jours;

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.

Possession de pornographie juvénile

Accessing child pornography

(4.1) Every person who accesses any child pornography is guilty of

(*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

(*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.

(4.1) Quiconque accède à de la pornographie juvénile est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de cinq ans, la peine minimale étant de quarante-cinq jours;

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.

Accès à la pornographie juvénile

Interpretation

(4.2) For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

(4.2) Pour l'application du paragraphe (4.1), accède à de la pornographie juvénile quiconque, sciemment, agit de manière à en regarder ou fait en sorte que lui en soit transmise.

Interprétation

Aggravating factor

(4.3) If a person is convicted of an offence under this section, the court that imposes the sentence shall consider as an aggravating factor the fact that the person committed the offence with intent to make a profit.

(4.3) Le tribunal qui détermine la peine à infliger à une personne déclarée coupable d'infraction au présent article est tenu de considérer comme circonstance aggravante le fait que cette personne a commis l'infraction dans le dessein de réaliser un profit.

Circonstance aggravante

Defence

(5) It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute

(5) Le fait pour l'accusé de croire qu'une personne figurant dans une représentation qui constituerait de la pornographie juvénile était âgée d'au moins dix-huit ans ou était présentée

Moyen de défense

child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.

comme telle ne constitue un moyen de défense contre une accusation portée sous le régime du paragraphe (2) que s'il a pris toutes les mesures raisonnables, d'une part, pour s'assurer qu'elle avait bien cet âge et, d'autre part, pour veiller à ce qu'elle ne soit pas présentée comme une personne de moins de dix-huit ans.

Defence

(6) No person shall be convicted of an offence under this section if the act that is alleged to constitute the offence

(*a*) has a legitimate purpose related to the administration of justice or to science, medicine, education or art; and

(*b*) does not pose an undue risk of harm to persons under the age of eighteen years.

(6) Nul ne peut être déclaré coupable d'une infraction au présent article si les actes qui constitueraient l'infraction :

a) ont un but légitime lié à l'administration de la justice, à la science, à la médecine, à l'éducation ou aux arts;

b) ne posent pas de risque indu pour les personnes âgées de moins de dix-huit ans.

Moyen de défense

Question of law

(7) For greater certainty, for the purposes of this section, it is a question of law whether any written material, visual representation or audio recording advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

1993, c. 46, s. 2; 2002, c. 13, s. 5; 2005, c. 32, s. 7.

(7) Il est entendu, pour l'application du présent article, que la question de savoir si un écrit, une représentation ou un enregistrement sonore préconise ou conseille une activité sexuelle avec une personne âgée de moins de dix-huit ans qui constituerait une infraction à la présente loi constitue une question de droit.

1993, ch. 46, art. 2; 2002, ch. 13, art. 5; 2005, ch. 32, art. 7.

Question de droit

Warrant of seizure

164. (1) A judge who is satisfied by information on oath that there are reasonable grounds for believing that

(*a*) any publication, copies of which are kept for sale or distribution in premises within the jurisdiction of the court, is obscene or a crime comic, within the meaning of section 163,

(*b*) any representation, written material or recording, copies of which are kept in premises within the jurisdiction of the court, is child pornography within the meaning of section 163.1, or

(*c*) any recording, copies of which are kept for sale or distribution in premises within the jurisdiction of the court, is a voyeuristic recording,

may issue a warrant authorizing seizure of the copies.

164. (1) Le juge peut décerner, sous son seing, un mandat autorisant la saisie des exemplaires d'une publication ou des copies d'une représentation, d'un écrit ou d'un enregistrement s'il est convaincu, par une dénonciation sous serment, qu'il existe des motifs raisonnables de croire :

a) soit que la publication, dont des exemplaires sont tenus, pour vente ou distribution, dans un local du ressort du tribunal, est obscène ou est une histoire illustrée de crime au sens de l'article 163;

b) soit que la représentation, l'écrit ou l'enregistrement, dont des copies sont tenues dans un local du ressort du tribunal, constitue de la pornographie juvénile au sens de l'article 163.1;

c) soit que l'enregistrement, dont des copies sont tenues, pour vente ou distribution, dans un local du ressort du tribunal, constitue un enregistrement voyeuriste.

Mandat de saisie

Summons to occupier

(2) Within seven days of the issue of a warrant under subsection (1), the judge shall issue a summons to the occupier of the premises requiring him to appear before the court and

(2) Dans un délai de sept jours après l'émission du mandat, le juge doit lancer une sommation contre l'occupant du local, astreignant cet occupant à comparaître devant le tribunal et à

Sommation à l'occupant

(*b*) in the forging or falsifying of credit cards.

b) falsifier des cartes de crédit ou en fabriquer des fausses.

Forfeiture

(2) Where a person is convicted of an offence under subsection (1), any instrument, device, apparatus, material or thing in relation to which the offence was committed or the possession of which constituted the offence may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Confiscation

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1), tout instrument, appareil, matière ou chose au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, en plus de toute peine applicable en l'espèce, être par ordonnance confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

Limitation

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 17; 2009, c. 28, s. 5.

Restriction

(3) Aucune ordonnance de confiscation ne peut être rendue en vertu du paragraphe (2) relativement à une chose qui est la propriété d'une personne qui n'a pas participé à l'infraction.

1997, ch. 18, art. 17; 2009, ch. 28, art. 5.

Unauthorized use of computer

342.1 (1) Every one who, fraudulently and without colour of right,

(*a*) obtains, directly or indirectly, any computer service,

(*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or

(*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Utilisation non autorisée d'ordinateur

342.1 (1) Quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;

b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa *a*) ou *b*) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur;

d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas *a*), *b*) ou *c*), ou en fait le trafic ou permet à une autre personne de l'utiliser,

est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Definitions

(2) In this section,

Définitions

(2) Les définitions qui suivent s'appliquent au présent article.

"computer password" « *mot de passe* »

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" « *programme d'ordinateur* »

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" « *service d'ordinateur* »

"computer service" includes data processing and the storage or retrieval of data;

"computer system" « *ordinateur* »

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(*a*) contains computer programs or other data, and

(*b*) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" « *données* »

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" « *dispositif électromagnétique, acoustique, mécanique ou autre* »

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" « *fonction* »

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" « *intercepter* »

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof;

"traffic" « *trafic* »

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.

« dispositif électromagnétique, acoustique, mécanique ou autre » "*electro-magnetic, acoustic, mechanical or other device*"

« dispositif électromagnétique, acoustique, mécanique ou autre » Tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une fonction d'un ordinateur, à l'exclusion d'un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale.

« données » "*data*"

« données » Représentations d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur.

« fonction » "*function*"

« fonction » S'entend notamment des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé des données de même que des fonctions de communication ou de télécommunication de données à destination, à partir d'un ordinateur ou à l'intérieur de celui-ci.

« intercepter » "*intercept*"

« intercepter » S'entend notamment du fait d'écouter ou d'enregistrer une fonction d'un ordinateur ou de prendre connaissance de sa substance, de son sens ou de son objet.

« mot de passe » "*computer password*"

« mot de passe » Donnée permettant d'utiliser un ordinateur ou d'obtenir des services d'ordinateur.

« ordinateur » "*computer system*"

« ordinateur » Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux :

a) contiennent des programmes d'ordinateur ou d'autres données;

b) conformément à des programmes d'ordinateur :

(i) soit exécutent des fonctions logiques et de commande,

(ii) soit peuvent exécuter toute autre fonction.

« programme d'ordinateur » "*computer program*"

« programme d'ordinateur » Ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction.

« service d'ordinateur » "*computer service*"

« service d'ordinateur » S'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données.

« trafic » "*traffic*"

« trafic » Le fait de vendre, d'exporter du Canada, d'importer au Canada ou de distribuer

un mot de passe, ou d'en disposer de quelque autre façon.

L.R. (1985), ch. 27 (1er suppl.), art. 45; 1997, ch. 18, art. 18.

Possession of device to obtain computer service

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(*b*) is guilty of an offence punishable on summary conviction.

Possession de moyens permettant d'utiliser un service d'ordinateur

342.2 (1) Quiconque, sans justification ou excuse légitime, fabrique, possède, vend, offre en vente ou écoule des instruments, ou des pièces de ceux-ci, particulièrement utiles à la commission d'une infraction prévue à l'article 342.1, dans des circonstances qui permettent de conclure raisonnablement qu'ils ont été utilisés, sont destinés ou étaient destinés à la commission d'une telle infraction, est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Forfeiture

(2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Confiscation

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1), tout instrument au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, en plus de toute peine applicable en l'espèce, être par ordonnance confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

Limitation

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 19.

Restriction

(3) Aucune ordonnance de confiscation ne peut être rendue en vertu du paragraphe (2) relativement à une chose qui est la propriété d'une personne qui n'a pas participé à l'infraction.

1997, ch. 18, art. 19.

Robbery and Extortion

Vol qualifié et extorsion

Robbery

343. Every one commits robbery who

(*a*) steals, and for the purpose of extorting whatever is stolen or to prevent or overcome resistance to the stealing, uses violence or threats of violence to a person or property;

(*b*) steals from any person and, at the time he steals or immediately before or immediately thereafter, wounds, beats, strikes or uses any personal violence to that person;

(*c*) assaults any person with intent to steal from him; or

Vol qualifié

343. Commet un vol qualifié quiconque, selon le cas :

a) vole et, pour extorquer la chose volée ou empêcher ou maîtriser toute résistance au vol, emploie la violence ou des menaces de violence contre une personne ou des biens;

b) vole quelqu'un et, au moment où il vole, ou immédiatement avant ou après, blesse, bat ou frappe cette personne ou se porte à des actes de violence contre elle;

c) se livre à des voies de fait sur une personne avec l'intention de la voler;

ary school unless the person is qualified as prescribed by the regulations.

Certificates

(2) Subject to this Act, a certificate of qualification as a teacher may be awarded only to a person of good moral character and physically fit to perform the duties of a teacher, who passes the examinations prescribed by, and otherwise complies with, the regulations.

Idem

(3) All certificates of qualification are valid for such periods as the regulations prescribe. R.S.O. 1980, c. 129, s. 233.

Termination of contract where welfare of school involved

263. Despite the other provisions of this Part and despite anything in the contract between the board and the teacher, where a permanent or probationary teacher is employed by a board and a matter arises that in the opinion of the Minister adversely affects the welfare of the school in which the teacher is employed,

(a) the board or the teacher may, with the consent of the Minister, give the other party thirty days written notice of termination, and the contract is terminated at the expiration of thirty days from the date the notice is given; or

(b) the board may, with the consent of the Minister, give the teacher written notice of immediate termination together with one-tenth of the teacher's yearly salary in addition to the amount to which the teacher would otherwise be entitled, and the contract thereupon is terminated. R.S.O. 1980, c. 129, s. 234.

Duties

Duties of teacher,

264.—(1) It is the duty of a teacher and a temporary teacher,

teach

(a) to teach diligently and faithfully the classes or subjects assigned to the teacher by the principal;

learning

(b) to encourage the pupils in the pursuit of learning;

religion and morals

(c) to inculcate by precept and example respect for religion and the principles of Judaeo-Christian morality and the highest regard for truth, justice, loyalty, love of country, humanity, benevolence, sobriety, industry, frugality, purity, temperance and all other virtues;

tions d'un enseignant dans une école élémentaire ou secondaire s'il ne possède pas la qualification requise, selon ce que prescrivent les règlements.

Brevet

(2) Sous réserve de la présente loi, le brevet de compétence d'enseignant ne peut être délivré qu'à la personne qui jouit d'une haute considération morale et d'une bonne santé lui permettant d'exercer ses fonctions d'enseignant, qui a réussi les examens prescrits par les règlements et qui se conforme à ceux-ci.

Idem

(3) Le brevet de compétence est valide pour la période précisée dans les règlements. L.R.O. 1980, chap. 129, art. 233.

Résiliation du contrat dans le cas où le bien de l'école est en jeu

263 Malgré les autres dispositions de la présente partie et malgré les dispositions du contrat entre le conseil et l'enseignant, si l'enseignant permanent ou stagiaire est employé par le conseil et qu'une question survient qui, de l'avis du ministre, nuit au bien de l'école où l'enseignant est employé :

a) le conseil ou l'enseignant peut, avec le consentement du ministre, donner à l'autre partie un préavis écrit de trente jours indiquant qu'il met fin à l'emploi et le contrat est résilié à l'expiration du délai de trente jours à compter de la date où l'avis est donné;

b) le conseil peut, avec le consentement du ministre, donner à l'enseignant un avis écrit indiquant qu'il met fin à l'emploi immédiatement, accompagné d'un dixième du salaire annuel de l'enseignant, en plus du montant auquel il a droit par ailleurs, sur quoi le contrat est résilié. L.R.O. 1980, chap. 129, art. 234.

Fonctions

Fonctions de l'enseignant :

264 (1) L'enseignant, même temporaire, exerce les fonctions suivantes :

enseignement

a) enseigner avec application et loyauté aux classes que lui assigne le directeur d'école, et enseigner ainsi les matières que lui assigne celui-ci;

apprentissage

b) encourager les élèves à poursuivre leur apprentissage;

religion et morale

c) inculquer, par les préceptes et l'exemple, le respect de la religion et les principes de la morale judéo-chrétienne et la plus haute considération pour la vérité, la justice, la loyauté, le patriotisme, l'humanité, la bienveillance, la sobriété, le zèle, la frugalité, la pureté, la modération et toutes les autres vertus;

co-operation

(d) to assist in developing co-operation and co-ordination of effort among the members of the staff of the school;

d) contribuer au développement de la collaboration et de la coordination des efforts entre les membres du personnel de l'école; collaboration

discipline

(e) to maintain, under the direction of the principal, proper order and discipline in the teacher's classroom and while on duty in the school and on the school ground;

e) faire respecter, sous la direction du directeur de l'école, le bon ordre et la discipline dans sa classe et, s'il est de service, à l'école et sur le terrain de l'école; discipline

language of instruction

(f) in instruction and in all communications with the pupils in regard to discipline and the management of the school,

(i) to use the English language, except where it is impractical to do so by reason of the pupil not understanding English, and except in respect of instruction in a language other than English when such other language is being taught as one of the subjects in the course of study, or

(ii) to use the French language in schools or classes in which French is the language of instruction except where it is impractical to do so by reason of the pupil not understanding French, and except in respect of instruction in a language other than French when such other language is being taught as one of the subjects in the course of study;

f) pour l'enseignement et les communications avec les élèves en ce qui concerne la discipline et le fonctionnement de l'école : langue d'enseignement

(i) utiliser l'anglais, sauf lorsque l'emploi de cette langue est impossible du fait que l'élève ne comprend pas l'anglais et sauf à l'égard de l'enseignement dans une langue autre que l'anglais quand cette autre langue est une des matières figurant au programme d'études,

(ii) utiliser le français dans les écoles ou les classes où le français est la langue d'enseignement, sauf lorsque l'emploi de cette langue est impossible du fait que l'élève ne comprend pas le français et sauf à l'égard de l'enseignement dans une langue autre que le français quand cette autre langue est une des matières figurant au programme d'études;

timetable

(g) to conduct the teacher's class in accordance with a timetable which shall be accessible to pupils and to the principal and supervisory officers;

g) enseigner conformément à un emploi du temps accessible aux élèves, au directeur et aux agents de supervision; emploi du temps

professional activity days

(h) to participate in professional activity days as designated by the board under the regulations;

h) participer aux journées pédagogiques telles qu'elles sont désignées par le conseil en application des règlements; journées pédagogiques

absence from school

(i) to notify such person as is designated by the board if the teacher is to be absent from school and the reason therefor;

i) aviser la personne désignée par le conseil s'il doit s'absenter de l'école et donner la raison de son absence; absence de l'école

school property

(j) to deliver the register, the school key and other school property in the teacher's possession to the board on demand, or when the teacher's agreement with the board has expired, or when for any reason the teacher's employment has ceased; and

j) remettre au conseil le cahier de présence, la clé de l'école et les autres objets appartenant à l'école qui sont en sa possession, à la demande du conseil ou à l'expiration de son entente avec celui-ci, ou à la cessation de son emploi pour quelque raison que ce soit; biens scolaires

textbooks

(k) to use and permit to be used as a textbook in a class that he or she teaches in an elementary or a secondary school,

(i) in a subject area for which textbooks are approved by the Minister, only textbooks that are approved by the Minister, and

k) n'utiliser et ne permettre d'utiliser comme manuel dans une classe d'école élémentaire ou secondaire où il enseigne : manuels

(i) que les manuels approuvés par le ministre dans une matière pour laquelle les manuels sont approuvés par ce dernier,

(ii) in all subject areas, only textbooks that are approved by the board. R.S.O. 1980, c. 129, s. 235 (1); 1982, c. 32, s. 58.

(ii) que les manuels approuvés par le conseil dans toutes les matières. L.R.O. 1980, chap. 129, par. 235 (1); 1982, chap. 32, art. 58.

Refusal to give up school property

(2) A teacher who refuses, on demand or order of the board that operates the school concerned, to deliver to the board any school property in the teacher's possession forfeits any claim that the teacher may have against the board.

Refus de rendre les biens scolaires

(2) L'enseignant qui refuse, à la demande ou sur l'ordre du conseil dont relève l'école visée, de lui remettre les biens scolaires qu'il a en sa possession, perd toute réclamation qu'il peut avoir contre le conseil.

Teachers, conferences

(3) Teachers may organize themselves for the purpose of conducting professional development conferences and seminars. R.S.O. 1980, c. 129, s. 235 (2, 3).

Conférence des enseignants

(3) Les enseignants peuvent s'organiser en vue de conférences et de séminaires ayant pour objet leur perfectionnement professionnel. L.R.O. 1980, chap. 129, par. 235 (2) et (3).

Duties of principal,

265. It is the duty of a principal of a school, in addition to the principal's duties as a teacher,

Fonctions du directeur :

265 En plus de ses fonctions d'enseignant, le directeur d'école exerce les fonctions suivantes :

discipline

(a) to maintain proper order and discipline in the school;

a) maintenir le bon ordre et la discipline dans l'école;

discipline

co-operation

(b) to develop co-operation and co-ordination of effort among the members of the staff of the school;

b) accroître la collaboration et la coordination des efforts entre les membres du personnel de l'école;

collaboration

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;

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;

inscription des élèves et cahier de présence quotidienne

pupil records

(d) to establish and maintain, and to retain, transfer and dispose of, in the manner prescribed by the regulations, a record in respect of each pupil enrolled in the school;

d) constituer, tenir à jour et conserver, de la manière prescrite par les règlements, un dossier pour chaque élève inscrit à l'école, le transférer ou s'en défaire;

dossiers scolaires

timetable

(e) to prepare a timetable, to conduct the school according to such timetable and the school year calendar or calendars applicable thereto, to make the calendar or calendars and the timetable accessible to the pupils, teachers and supervisory officers and to assign classes and subjects to the teachers;

e) préparer un emploi du temps, diriger l'école en fonction de cet emploi du temps et du calendrier ou des calendriers de l'année scolaire qui s'y applique, permettre aux élèves, aux enseignants et aux agents de supervision d'avoir accès à ce calendrier ou ces calendriers et à l'emploi du temps, et assigner les classes et les matières aux enseignants;

emploi du temps

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;

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 majeur;

examens et bulletins scolaires

promote pupils

(g) subject to revision by the appropriate supervisory officer, to promote such pupils as the principal considers proper and to issue to each such pupil a statement thereof;

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;

passage des élèves

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;

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;

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;

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;

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;

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;

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;

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;

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;

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;

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

accès à l'école ou à la classe

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;

visitor's book

(n) to maintain a visitor's book in the school when so determined by the board. R.S.O. 1980, c. 129, s. 236.

registre des visiteurs

n) tenir un registre des visiteurs dans l'école si le conseil le prescrit. L.R.O. 1980, chap. 129, art. 236.

Pupil Records

Dossier d'élève

Definition

266.—(1) In this section, except in subsection (12), "record" in respect of a pupil means a record maintained or retained by the principal of a school in accordance with the regulations and the guidelines issued by

Définition

266 (1) Pour l'application du présent article, à l'exception du paragraphe (12), le terme «dossier», relativement à un élève, désigne le dossier tenu ou conservé par le directeur d'école conformément aux règlements et aux lignes directrices du ministre.