WARNING

The President of the panel hearing this appeal directs that the following should be attached to the file:

An order restricting publication in this proceeding under ss. 486(1), (2), or (3) of the *Criminal Code* shall continue. These sections of the *Criminal Code* provide:

486. (1) Any proceedings against an accused shall be held in open court, but the presiding judge or justice may order the exclusion of all or any members of the public from the court room for all or part of the proceedings if the judge or justice is of the opinion that such an order is in the interest of public morals, the maintenance of order or the proper administration of justice or is necessary to prevent injury to international relations or national defence or national security.

(2) For the purpose of subsection (1), the "proper administration of justice" includes ensuring that.

(a) the interests of the witnesses under the age of eighteen years are safeguarded in all proceedings; and

(b) justice system participants who are involved in the proceedings are protected.

(3) If an accused is charged with an offence under section 151, 152, 153, 153.1, 155 or 159, subsection 160(2) or (3) or section 163.1, 171, 172, 172.1, 173, 212, 271, 272 or 273 and the prosecutor or the accused applies for an order under subsection (1), the judge or justice shall, if no such order is made, state, reference to the circumstances of the case, the reason for not making an order. R.S., c. C-34, s. 442; 174-75-76, c. 93, s. 44; 1980-81-82-83, c. 110, s. 74, c. 125, s. 25; R.S.C. 1985, c. 19 (3rd Supp.), s. 14; c. 23 (4th Supp.), s. 1; 1992, c. 21, s. 9; 1993, c. 45, s. 7; 1997, c. 16, s. 6; 1999, c. 25, s. 2; 2001, c. 32, s. 29; 2001, c. 41, s. 16, 34 and 133(13), (14); 2002, c. 13, s. 20; 2005, c. 32, s. 15; 2005, c. 43, ss. 4 and 8(3)(a).

CITATION: R. v. Cole, 2011 ONCA 218
DATE: 20110322
DOCKET: C50526

COURT OF APPEAL FOR ONTARIO

Winkler C.J.O., Sharpe and Karakatsanis JJ.A.

BETWEEN

Her Majesty the Queen

Respondent

and

Richard Cole

Applicant/Appellant

Frank Addario and Andrew Furgiuele, for the appellant

Amy Alyea, for the respondent

Heard: November 22, 2010

On appeal from the order of Justice P. Kane of the Superior Court of Justice dated April 28, 2009, with reasons reported at 2009 CanLII 20699 (ON S.C.), allowing an appeal from the order of Justice André L. Guay of the Ontario Court of Justice dated May 12, 2008, with reasons reported at [2008] O.J. No. 2417 (C.J.).

Karakatsanis J.A.:

[1] The main issue in this appeal is whether the appellant, a high-school teacher, had a reasonable expectation of privacy in the contents of a work computer on which he was entitled to store personal information.

[2] The appellant was charged with possession of child pornography and unauthorized use of a computer contrary to ss. 163.1(4) and 342.1(1) of the *Criminal Code*. A computer technician at the school accessed, through the school server, the contents of the teacher's laptop and found nude sexually explicit images of a grade 10 student on the hard drive. He advised the principal, who directed the technician to copy the images onto a disc and required the appellant to give him the laptop. A school board official searched the laptop and copied temporary internet files from the appellant's surfing history onto another disc. The two discs and the laptop were turned over to the police, who searched them without a warrant.

[3] The matter was tried at the Ontario Court of Justice. On a pre-trial application, the trial judge excluded the evidence pursuant to s. 24(2) of the *Charter*, finding that the police had infringed the appellant's s. 8 rights because he had a reasonable expectation of privacy in the laptop's contents. On summary conviction appeal to the Superior Court of Justice, the appeal judge overturned the trial judge's decision and sent the matter back for a retrial. The appeal judge found the appellant had no reasonable expectation of privacy in his laptop.

[4] On appeal to this court, the appellant submits that the summary conviction appeal judge erred in finding that the teacher had no reasonable expectation of privacy in the laptop; that both the technician's and the police officer's search was a breach of s. 8 of

the *Charter*; and that the evidence should be excluded under s. 24(2) in accordance with the reasons of the trial judge.

[5] This appeal raises the following issues:

1. Did the appellant have a reasonable expectation of privacy in the contents of the laptop?
2. If so, did (a) the technician or (b) the principal or (c) the school board breach s. 8 of the *Charter*?
3. Did the police breach s. 8 of the *Charter* by searching the laptop and the compact discs without a warrant?
4. If so, did the trial judge err in excluding the evidence?

[6] For the reasons that follow, I conclude that the appellant had a reasonable expectation of privacy from state intrusion in the personal use of his work computer and in the contents of his personal files on its hard drive. However, his expectation of privacy was modified. He had no expectation of privacy with respect to access to his hard drive by his employer's technician for the limited purpose of maintaining the technical integrity of the school's information network and the laptop.

[7] Assuming, as I have, that the *Charter* applies to the school board, I have concluded that the search by the technician, the principal and the school board officials did not breach s. 8 of the *Charter*. The technician was acting within the scope of his functions when he came across the student photographs and thus did not violate the appellant's modified privacy interests. The principal and school board officials acted

reasonably under the authority of the *Education Act* to protect students and a safe learning environment.

[8] However, the police search of the laptop and the police seizure of the disc containing temporary internet files from the appellant's browsing history violated the appellant's right to be secure against unreasonable search and seizure. I agree with the trial judge's conclusion that this evidence should be excluded under s. 24(2) of the *Charter*.

[9] Different considerations apply to the disc containing the photographs delivered by the principal to the police. This evidence, like photographs in an envelope, did not require further search by police and the appellant had no continuing personal privacy interest in the images of the student obtained through the school system. As a result, there was no police search or seizure of this evidence within the meaning of s. 8 of the *Charter*.

[10] For the reasons that follow, I would grant leave to appeal and I would allow the appeal, set aside the decision of the summary conviction appeal judge, substitute an order excluding the evidence of the disc containing the temporary internet files and the laptop and its mirror image, and remit the matter back to the Ontario Court of Justice for trial.

Background Facts

[11] The appellant was provided with a laptop by his school for use in teaching communication technology and in supervising a laptop program for students. He was a

sitting member of the school's technology committee and was one of several individuals with domain administration rights to the network, so that he could monitor and police the network. As a supervisor, he had authority to remotely access the data stored on student computers connected to the school network, and he did so regularly as part of his employment. The appellant accessed a student's email account, found nude photographs of another student and copied them onto the hard drive of his school-issued laptop.

[12] A computer technician employed by the school also had domain administration rights as part of his responsibility for monitoring and maintaining the integrity and stability of the school network. Using new software, he observed a large amount of activity between the appellant's laptop and the school's server so he remotely accessed the appellant's hard drive to perform a virus scan and verify the system's integrity. In doing so, the technician accessed a hidden folder on the hard drive. The hidden folder contained nude, sexually explicit images of a girl who the technician believed to be an underage student at the school.

[13] The technician took a screen shot of the laptop to preserve the window with the appellant's name, the path to the location of the pictures and some thumbnail pictures of the images. He confirmed that the girl was a student and reported it to the principal. The principal wanted to confirm that the girl was a student so the technician again accessed the appellant's hard drive through the server and showed the principal only the face in the photographs. The principal asked the technician to copy the photos onto a disc and not to

discuss it with anyone. The technician copied the screen shot and the photographs onto a disc and gave it to the principal.

[14] The next morning, the principal asked the appellant to hand over the computer and to provide his password and contact information. The appellant did not provide his password but advised the principal that technicians would not require the password to access the computer. That same day, one of the school board's technicians subsequently accessed and searched the appellant's computer. He copied temporary internet files which had been in the browsing history of the laptop and placed them onto a disc. Those files contained large numbers of pornographic images.

[15] The principal and school board officials gave police the laptop and the compact discs. An officer in the cyber-crime unit was assigned to investigate. The school board advised the officer that the laptop belonged to the school board. The officer was aware that teachers stored personal information on their laptops. He was provided with copies of the policies and letters indicating that teachers had personal information on their computers. However, the officer did not believe the data belonged to the appellant. The officer viewed the discs to determine whether, in his opinion, the photographs constituted child pornography. The appellant was subsequently arrested. Some weeks later, the officer sent the laptop for analysis. He did not obtain a search warrant.

[16] The laptop was owned by the school board. However, the appellant in fact had exclusive use and possession of the laptop and protected access to the laptop by use of a

password. Teachers were permitted to use their computer for personal use and to take it home during weekends and vacations.

[17] A Policy and Procedures Manual, prepared by the school board for all of its teachers, permitted personal use of the computer. The policy provided there was to be no inappropriate content on the school computer, including sexually explicit material. Section P9.06 of the policy provided that "all data and messages generated on or handled by Board equipment are considered to be the property of the Rainbow District School Board and not the property of the users of the technology." In addition, the policy mandated that:

> Rainbow 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.

[18] However, the policy did not provide for the search of the computers nor did it address the issue of privacy, except as it related to email. Under "email", a separate privacy subsection states that the administrative team can "legally open private email if that action seems necessary for the ongoing 'health' of the system or if inappropriate use is suspected. *In cases where access to a user's account for system/trouble-shooting purposes is required, attempts to request the user's permission will be made first*" (Emphasis in original).

[19] Students were required to sign an Acceptable Use Agreement (AUA) that regulated the use of laptops by students. Under this agreement, students were advised: "Teachers and administrators may monitor all student work and email 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." The AUA was not signed by teachers or staff. However, the principal had advised the staff at several staff meetings that whatever rules applied to students also applied to staff.

[20] The appellant had stored photographs of his wife on his computer. When he turned over the computer, the appellant asked the principal not to access the folder with photos of his wife. When the principal asked for the password, the appellant declined to give it to the principal. Another teacher wrote to the principal advising that a privacy policy for teachers' laptops was needed: teachers "often have sensitive information about students on their computers that may not be appropriate for IT staff to read". He stated that, like many other teachers, he had personal information on his laptop. There was evidence that the teachers maintained personal information on their computers, including bank account numbers and financial data.

The Trial Judge's Decision

[21] The trial judge held that the appellant had a reasonable expectation of privacy in the contents of his laptop hard drive. He found that whatever the official policy was, the school board's actual policy was that staff members could load private material onto their

computers and they had exclusive use of the computers, including weekends and summers.

[22] The trial judge stated that this case was very similar to *R. v. Buhay*, [2003] 1 S.C.R. 631, in which the Supreme Court of Canada concluded that the police's warrantless search of the accused's rented locker violated the accused's reasonable expectation of privacy. He reasoned that the appellant's computer was similar to an office desk or a rented locker and that the appellant's password was analogous to a key.

[23] The trial judge held that the *Charter* did not apply to the school board and that the principal was entitled to hand over the material to the police. He held, however, that the warrantless search and seizure of the material by the police officer constituted a breach of the appellant's s. 8 *Charter* rights.

[24] The trial judge found that the police had ample time to secure a warrant and that they wrongly concluded that the school board's property interest in the laptop trumped any personal interest or expectation of privacy that the appellant may have had in the laptop's contents. In doing so, he determined that the evidence should be excluded under s. 24(2) of the *Charter*.

The Summary Conviction Appeal Judge's Decision

[25] The summary conviction appeal judge found that the trial judge erred in law when he concluded that the appellant had a reasonable expectation of privacy in the contents of the laptop's hard drive.

[26] The appeal judge outlined the contextual factors in *R. v. Edwards*, [1996] 1 S.C.R. 128 which are to be considered in assessing whether the appellant had a reasonable expectation of privacy in his laptop. He was prepared to accept that the appellant had a subjective expectation of privacy. However, he found that the facts surrounding the appellant's employment demonstrated that any subjective expectation of privacy was not objectively reasonable. He found that the terms of the AUA and the terms of the board's policies were terms of the appellant's employment. As such, the appellant agreed to his employer's right to monitor his work, email and data stored on his computer drive and therefore waived his right of privacy to this data.

[27] Furthermore, the appeal judge found that given the appellant's supervisory role on the IT committee, his role in enforcing the policies and agreements, and his knowledge that the employer regularly accessed information on computers connected to the network and that the school could bypass any password protection, it could not be said that the appellant's expectation of privacy in relation to the data he stored on his laptop was objectively reasonable.

[28] The appeal judge concluded that the lack of a reasonable expectation of privacy did not change upon the employer delivering the data to the police. As a result, the appeal judge allowed the appeal, set aside the decision of the trial judge and remitted the matter back for trial.

ANALYSIS

I. Did the appellant have a reasonable expectation of privacy in the contents of the laptop?

[29] The appellant submits that the summary conviction appeal judge erred in his analysis by relying upon an employment contract framework and by failing to review the extent to which written policies were modified by convention and usage. In particular, the appellant submits that in order to displace an expectation of privacy that arises from the permission to use the laptop for personal use and the exclusive possession of the laptop, there should be a written policy that clearly provides for random, 'standardless' searches.

[30] The respondent submits that the summary conviction appeal judge correctly assessed all the factors in *Edwards* and correctly concluded that the appellant had no reasonable expectation of privacy in the files on his laptop.

[31] In order to establish that a person's privacy rights have been violated, the person must first establish the existence of a reasonable expectation of privacy. The reasonable

expectation of privacy must be determined based on a totality of the circumstances, including the factors identified in *Edwards*, at para. 45:

- whether the accused was present at the time of the search;
- whether the accused had possession or control of the property or place searched;
- whether the accused owned the property or place searched;
- the historical use of the property or item;
- the ability to regulate access, including the right to admit or exclude others from the place;
- the existence of a subjective expectation of privacy; and
- the objective reasonableness of the expectation.

[32] More recently, in *R. v. Tessling*, [2004] 3 S.C.R. 432, at para. 32, and *R. v. Patrick*, [2009] 1 S.C.R. 579, at para. 27, the Supreme Court of Canada set out an analytical framework for assessing the totality of the circumstances, which involves consideration of the nature or subject matter of the evidence gathered, whether the applicant had a direct interest in that subject matter, whether the applicant had a subjective expectation of privacy in the subject matter, and whether that expectation of privacy was objectively reasonable.

[33] In *Tessling* at paras. 20-24, the court noted that in determining the reasonableness of the privacy expectation, it is a useful analytical tool to determine the nature of the privacy interest. In this case, the search involved both a territorial privacy interest in the

hard drive of a computer used in part for personal use, and an informational privacy interest, including potentially intimate details of the lifestyle and personal choices of the appellant that can have a bearing on his "dignity, integrity and autonomy" (*R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293).

[34] In *Patrick*, Binnie J. observed at para. 17 that an asserted expectation of privacy in things located on someone else's property must be one that an independent and informed observer is prepared to recognize as reasonable. Whether an expectation is objectively reasonable includes: the nature of the place where the search occurred; whether the informational content of the subject matter was in public view, had been abandoned, or was already in the hands of third parties; whether the police technique was intrusive in relation to the privacy interest; whether the evidence gathering technique was objectively unreasonable; and whether the informational content exposed intimate details of the appellant's lifestyle or information of a biographic nature (see *Patrick*, at para. 27).

[35] I turn first to the *Edwards* factors.

[36] Given the remote nature of an electronic search, the accused's presence during such a search will ordinarily not be a significant factor. 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.

[37] The appellant actually used the laptop for personal use as evidenced by the presence of photographs of his wife. He had the right to keep the laptop in his possession and he protected access to the computer by a password. The appeal judge accepted that the appellant had a subjective expectation of privacy.

[38] 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.

[39] Furthermore, there was no clear privacy policy relating to teachers' laptops. The only privacy provision in the Policy and Procedures Manual related to email; it emphasized that attempts would be made to request the user's permission if access was required for system/trouble-shooting purposes. It did not provide for the monitoring or search of the teachers' laptops.

[40] The trial judge did not make a finding, and the parties did not agree, on whether the AUA regulating the use of student laptops also applied to teachers. The AUA was signed by the students but not by the teachers. While the appeal judge accepted the principal's testimony that he had advised teachers that all student policies applied to teachers as well, the terms of the AUA do not readily translate into a privacy policy for teachers. For example, under this agreement, students were advised: "Teachers and administrators may monitor all student work and email 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." This is not consistent with the policy provisions relating to teachers' emails. Nor was this term absolute: even the technician recognized that students had privacy interests that precluded him from reading information that pertained to students.

[41] There can be no doubt that the appellant was aware of the school policies and the AUA, given his membership in the IT committee. Furthermore, he was aware that others with domain administration rights to the network could access a laptop connected to the system since he did so regularly as part of his role to police student use of their laptops. However, there was no evidence that anyone monitored or policed the teachers' use of their laptops, nor did the AUA or the Policy and Procedures Manual address this issue. Furthermore, to the extent that the terms of the AUA applied to teachers, the evidence shows that they were modified by the policy and by convention and usage of the teachers' laptops.

[42] Finally, the fact that a computer technician could access the hard drives of the laptops does not negate a reasonable expectation of privacy, just as the existence of a master key does not destroy the reasonable expectation of privacy in a rented apartment or in a bus locker. In *Buhay*, the Supreme Court noted that the absence of an exclusive right of access did not undermine an expectation of privacy.

[43] Similarly, this court has held that a hotel guest's awareness that cleaning staff will enter the room does not remove an individual's reasonable expectation of privacy in a hotel room. In *R. v. Kenny* (1992), 52 O.A.C. 70, leave to appeal to S.C.C. refused, [1992] S.C.C.A. No. 231, Arbour J.A. stated at para. 14:

> Objects not left in plain view or stored in areas which do not require daily maintenance, such as inside drawers, closets, toiletry bags, briefcases and suitcases, can be reasonably expected to remain private despite access to the room by hotel staff for cleaning purposes…Privacy would be inadequately protected if the reasonableness of a given expectation of privacy in one's office or hotel room could be displaced by an awareness of the possibility that cleaning staff may rummage through anything that is not locked away.

Although the hotel gave consent to the police to search the accused's hotel room after cleaning staff found evidence of drug trafficking, this court concluded that the search of a rented hotel room by police requires prior judicial authorization, based on the reasonable expectation of hotel guests that their belongings left inside their room will be sheltered from uninvited state scrutiny.

[44] There is little authority in Canada on the issue of whether an individual has a reasonable expectation of privacy in work computer. In *R. v. Little*, 2009 CanLII 41212 (ON S.C.), the application judge held that the accused had a reasonable expectation of privacy in the information on his work hard drive, but it was a diminished expectation compared to that in a home computer or a computer owned and used exclusively by an individual running his or her own business. In *France (Republic) v. Tfaily* (2009), 98

O.R. (3d) 161 (C.A.) [In Chambers], an application for leave to appeal, the question raised on appeal was whether there were sufficient grounds to issue warrants to search for the applicant's work computers. The applicant was a professor at Carleton University. Simmons J.A. noted that university professors are entitled to use their work computers for personal communications and research and that therefore they have an objectively reasonable expectation of privacy in relation to personal electronic data.

[45] I agree with the trial judge that, based upon the totality of the circumstances in this case, including the factors set out in *Edwards*, the appellant had a reasonable expectation of privacy in the personal use of his work laptop. Although this was a work computer owned by the school board and issued for employment purposes with access to the school network, the school board gave the teachers possession of the laptops, explicit permission to use the laptops for personal use and permission to take the computers home on evenings, weekends and summer vacation. The teachers used their computers for personal use, they employed passwords to exclude others from their laptops, and they stored personal information on their hard drives. There was no clear and unambiguous policy to monitor, search or police the teachers' use of their laptops.

[46] Furthermore, applying the factors in *Patrick* at para. 27, the information in the folder stored on the hard drive was not in public view, was not abandoned and was not in the hands of third parties. While the access by the technician for the purpose of maintaining the integrity of the system was not intrusive or objectively unreasonable,

access by a state actor for the purpose of determining the nature of the information stored by the appellant would be intrusive. Access to that information on the hard drive potentially exposed intimate details of the appellant's personal choices and could have exposed intimate details of a personal nature. The appellant had a reasonable expectation of privacy in both the hard drive of the laptop and the personal information it contained.

[47] On the other hand, the appellant knew that a school technician had a limited right of access to the hard drive as part of his duties to maintain the stability and security of the network system. Business and other institutions commonly engage technicians to service and maintain their networks. Users understand that a technician can access computers connected to the network to ensure the integrity of the system. The appellant's reasonable expectation of privacy was modified to the extent that the appellant knew that his employer's technician could and would access the laptop as part of his role in maintaining the technical integrity of the school's information network. However, this was not sufficient to displace a reasonable expectation that otherwise would exist in the personal electronic information maintained on his hard drive, except to that extent and for that limited purpose.

[48] I conclude, therefore, that the appellant had a reasonable expectation of privacy in the information stored in the hard drive of his laptop, which was subject to the limited right of access by his employer's technicians performing work-related functions. In other

words, the appellant had no expectation of privacy with respect to this limited type of access.

2(a). Did the technician's search engage s. 8 of the *Charter*?

[49] The trial judge found that the technician and the school board were not subject to the *Charter*. The summary conviction appeal judge found it unnecessary to deal with the issue given his finding that there was no reasonable expectation of privacy.

[50] On this appeal, the Crown concedes that the school board was subject to the *Charter* but maintains that the technician's actions did not engage s. 8. For the purposes of this appeal, I am assuming that the *Charter* applies to the school board. A similar assumption was made in *R. v. M.R.M.*, [1998] 3 S.C.R. 393, at para. 25, where Cory J. held that in light of the concession made by the Crown, it would be best to assume for the purposes of the case that the *Charter* applied to the actions of the vice-principal.

[51] The appellant argues that the technician's search of the contents of his hard drive went beyond his role of maintaining the integrity of the school's information network and his implied right of access. The appellant suggests that it was not sufficient that the technician acted on a "hunch" that does not qualify as credibly based probability and that the technician was required to have reasonable grounds to search the content of the laptop's hard drive.

[52] As noted by Cory J. in *Edwards* at para. 45, the right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated. As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused established a reasonable expectation of privacy that his personal information will not be accessed? Second, if he has such an expectation, was the search by the state actor conducted reasonably?

[53] Thus, the first inquiry in the case of the technician's search is whether the appellant had a reasonable expectation of privacy with respect to the technician's limited right of access to the laptop. If not, s. 8 of the *Charter* is not engaged. If the technician was acting outside the scope of his duties when conducting the search, then the analysis shifts to the second stage to assess the reasonableness of the technician's search.

[54] In assessing the scope and purpose of the technician's actions, the appellant's submission that the technician was required to have reasonable and probable grounds, or a reasonable suspicion of illegal activity, is misplaced. The issue of whether the search was conducted reasonably does not arise at this stage of the analysis. Furthermore, such a standard would severely hinder a technician's ability to service and oversee the technical integrity of the school's network. Provided he acted for this purpose, the technician would be within his implied right of access.

[55] The technician did not set out to target the appellant or his computer, and he was not searching for any personal information. The technician testified that he was

responsible for maintaining the stability and integrity of the network. He was checking the system with new software that reported on activity on the network and the computers attached to it. He was accessing the appellant's computer remotely because he had observed a large amount of activity between the appellant's laptop and the school's server, which could have been caused by a virus, but he was not sure what the cause was. He testified that he was also concerned because the appellant had affected the stability of the server in the past. He was going to perform a virus scan on the appellant's "My Documents" folder in order to see if the system's integrity was being compromised, when he came across a hidden folder called "New Folder". Although most users would not be able to see a hidden folder, the technician had his computer set to reveal hidden folders. Knowing that such folders are not necessarily created by the user, and in the context of searching for the reason for the extraordinary activity, the technician accessed the folder to find out what it contained. When he opened the hidden folder, the numerous explicit nude thumbnail images of a girl he believed was an underage student at the school were in plain view.

[56] Although the trial judge characterized the technician's search of the appellant's laptop as a "free range search", he did not make findings on the nature of the technician's access, as it was not necessary given his finding that the *Charter* did not apply to the school board.

[57] The evidence in this case indicates that the technician was not simply ‘rummaging’ in the hard drive. Any curiosity on the part of the technician related to the stability of the system and not to information about the appellant or the information he had stored. The technician articulated a specific reason for opening the folder that directly related to his role of maintaining the network. Once the folder was open, the thumbnail photographs were in plain view and the nature of the photographs was readily apparent. This was not a folder that contained personal written information that would have engaged a further level of examination.

[58] On these facts, I am satisfied that the technician was accessing the appellant’s laptop for the limited purpose of maintaining the network. The technician found the images in the course of his legitimate access to the computer. Therefore, the appellant had no expectation of privacy with respect to this limited type of action. Since there was no reasonable expectation of privacy with respect to the technician’s actions, s. 8 of the *Charter* was not engaged.

[59] Having opened the file and discovered the sexually explicit photographs of someone he believed was an underage student, the technician acted reasonably in taking a screen shot, confirming that the girl was a student and contacting the principal.

2(b). Did the principal's search breach s. 8 of the *Charter*?

[60] The parties focused their submissions on the conduct of the technician. However, as discussed above, the appellant had a reasonable expectation of privacy as a result of his personal use of the computer and would not expect that state agents would have the unrestricted right to view his personal files. Therefore, assuming that the school board and its employees are subject to the *Charter*, the actions of the principal in viewing the face in the photographs, directing the technician to copy the photographs onto a disc and requiring the appellant to immediately hand over the laptop, constituted a search and seizure within the meaning of s. 8 of the *Charter*.

[61] I agree with the trial judge's finding that the principal had the overriding obligation to ensure the health and safety of the students and once the information was disclosed to him, he had no choice but to take appropriate action.

[62] In *M.R.M.* at para. 47, Cory J. noted that teachers and principals must be able to act quickly to protect their students and to provide the orderly atmosphere required for learning. The Supreme Court of Canada noted that a school official should not be held to the same stringent standard as police when conducting searches of students. The principal had a statutory duty under s. 265 of Ontario's *Education Act*, R.S.O. 1990, c. E.2 to ensure a safe school environment, which implies an authority to conduct reasonable searches and seizures within his school without prior judicial authorization to fulfill that duty:

> 265. (1) It is the duty of a principal of a school, in addition to the principal's duties as a teacher,
>
> *discipline*
>
> (a) to maintain proper order and discipline in the school;
>
> . . .
>
> *care of pupils and property*
>
> (j) to give assiduous attention to the health and comfort of the pupils, … to the care of all teaching materials and other school property…;
>
> . . .
>
> *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…

[63] The principal acted quickly to investigate a teacher's possession of sexually explicit photographs of a grade 10 student in his school. Searching the laptop to confirm the identity of the girl in the pictures, seizing evidence by making a copy of the images onto a disc and seizing the laptop computer from the appellant were all implicitly authorized by law: see s. 265 of the *Education Act* and *M.R.M.* There is no suggestion that the law is not reasonable or that the search and seizures by the principal were not carried out reasonably (*R. v. Collins*, [1987] 1 S.C.R. 265, at p. 278). Therefore, there was no violation of s. 8 of the *Charter* by the principal.

2(c). Did the school board's search breach s. 8 of the *Charter*?

[64] While the laptop was still in the possession of the school board, officials ultimately gained access without the password and searched the laptop, obtained data relating to the appellant's internet browsing, and saved the 'temporary internet files' onto a disc. The principal considered it a "board matter", "investigating teacher conduct". Obviously, the school board was investigating a serious allegation of teacher misconduct and a threat to the school environment. Officials chose to search the laptop and secure further evidence before handing the laptop over to the police. While there was no longer any immediate threat to the school, its students or the school's computer network, the school board had an ongoing obligation to take steps to ensure a safe and secure learning environment for its students and to protect the students' privacy rights. The search of the laptop and preservation of the evidence for an internal discipline procedure was an obvious means to do so. Although there was no suggestion that the images copied from the temporary internet files depicted any student or were obtained from the school network, presumably they would be evidence potentially relevant to the purpose of the appellant's possession of the student's photographs or to whether this use of the computer contravened the school board's Policy and Procedures Manual.

[65] In *M.R.M.*, Cory J. stated at para. 1 that:

> 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.

With this in mind, the court noted at paras. 48 and 50 that the search of a student by a principal is reasonable if the principal has reasonable grounds to believe that school regulations have been breached and that a search would reveal evidence of that breach. Although that case dealt with the conduct and search of a student, it would apply with equal force to the conduct and search of a teacher (involving a school computer and the school network) that threatened the well-being of students. On the basis of the record in this case, I am satisfied that this further search and seizure by the school board was authorized and reasonable.

[66] The appellant made no submissions relating to the search of the laptop by the school board. I see 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.

3. Did the police violate s. 8 of the *Charter* by searching the laptop and the compact discs?

[67] When the school board turned over the discs and the laptop to the police, the investigating officer - a specialist in the 'cyber-crime unit' - looked at the images on the discs to satisfy himself that the pictures constituted child pornography. A few weeks

later, he sent the laptop to another police force where a mirror image was taken of the laptop's hard drive, affording the police a view of the entire contents of the laptop. Once the police had the laptop in their possession, there was no urgency and no exigent circumstances and a warrant could easily have been obtained.

[68] The police officer testified that he did not obtain a search warrant because the computer was owned by the school board and was a 'staff computer', and he apparently believed he had the consent of the school board to search it.

[69] As discussed above, ownership of the item seized or the place to be searched is just one consideration in determining whether a privacy interest exists and does not extinguish an individual's reasonable expectation of privacy. To the extent that the appellant's reasonable expectation of privacy was modified by the technician's implied right of access in relation to maintaining the school's network, this would not extend to a police intrusion to investigate a criminal offence without a warrant. The technician's discovery of the photographs during the course of his implied right of access did not vitiate the appellant's reasonable expectation of privacy in the contents of his laptop in relation to the police. Although the laptop and some of the personal information was in the hands of a third party - the employer - as a result of the technician's access, the appellant did not abandon his privacy interest in the personal information on the computer. Furthermore, the police technique was intrusive in copying the entire contents of the hard drive. The contents of the hard drive of a laptop may contain extremely

personal information such as medical and financial reports, personal journals, emails and appointments.

[70] Nor was the officer justified in relying upon the consent of the school board to search the work computer. In considering the issue of third party consent, this court held in *Kenny* that a mistake of law relating to the hotel manager's ability to consent did not justify the police search without a warrant. Arbour J.A. referenced American constitutional jurisprudence and the U.S. Supreme Court's decision in *Stoner v. California*, 84 S.Ct. 889 (1964). In that case, the court recognized that a hotel guest gives express or implied consent to cleaning staff to enter the room in the guest's absence in the performance of their duties, but the court refused to permit an otherwise unlawful police search of a hotel room to rest upon the consent of the proprietor.

[71] The leading American decision is *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), writ of certiorari denied: 552 U.S. 1105 (2008). In that case, the employer discovered that the company computer, provided to the defendant for his business use, had been used to access child pornography websites. The company gave the police its consent to open the defendant's private office and to search the company computer.

[72] The Court of Appeals for the Ninth Circuit held that the use of a password on the defendant's computer and the lock on his private office door were sufficient evidence of a subjective expectation of privacy. The court also held that the employer could give valid consent to a search of the contents of the hard drive of the defendant's workplace

computer because the computer was the type of workplace property that remained within the control of the employer, even if the defendant had placed personal items on it. The court took the following factors into consideration: the information technology department had complete administrative access to all employee computers; the company had installed a firewall which monitored the flow of internet traffic; employees' internet usage was routinely monitored and reviewed on a daily basis; employees were apprised of the company's monitoring efforts through training and an employment manual; and the employees were told that the computers were company-owned and not to be used for activities of a personal nature. Based on these factors, the court in *Ziegler* held that the warrantless search of the defendant's work computer was justified by the employer's "consent" to the search.

[73] However, most of these factors are not found in the present case. In particular, the appellant and other teachers at the school were expressly permitted to store personal information on their work computers. Accordingly, the school board did not have the authority to consent to the search of a work laptop in which they had permitted personal use by the teacher.

[74] It also makes no difference that the computer was lawfully seized by one state actor - the school officials - and then turned over to another state actor - the police - who engaged in a criminal investigation: see e.g. *R. v. Colarusso*, [1994] 1 S.C.R. 20; and *R. v. Jarvis*, [2002] 3 S.C.R. 757. In *Colarusso*, a coroner seized the blood of the accused

under the authority of the provincial *Coroners Act*, R.S.O. 1990, c. C.37 and then gave the blood to the police to have analyzed. The Supreme Court of Canada held that the police were not entitled to use the blood sample for the purpose of a criminal prosecution. La Forest J., speaking for the majority, said at pp. 66-67:

> I do not believe that the criminal law enforcement arm of the state should be able to "piggy-back" the coroner's investigation and appropriate evidence obtained by a coroner under s. 16 of the *Coroners Act*. While a coroner may be able to seize evidence without prior judicial authorization, the criminal law enforcement arm of the state must continue to comply with the *Hunter* requirements throughout its investigation.
>
> **…** To permit such evidence to be appropriated by the state and thereby circumvent the *Hunter* requirement of prior authorization would be to limit unduly the privacy rights guaranteed by s. 8 of the *Charter*. In keeping with the purposive approach applied by this Court in past s. 8 jurisprudence, it is essential to ensure that the coroner's investigative powers are tempered in such a way as to ensure that the information derived by a coroner's investigation will not be used to circumvent the procedural requirements outlined in *Hunter* and thereby unfairly incriminate the appellant.

[75] In *R. v. Dyment*, [1988] 2 S.C.R. 417, a doctor provided the police with a blood sample that had been taken for medical purposes after a motor vehicle accident. The Supreme Court of Canada held that the accused may have impliedly consented to a sample being taken for medical purposes but that he retained an expectation that his privacy interest in the sample would continue past the time of its taking. Therefore, the court held that in taking the blood sample and analyzing the blood alcohol content

without a warrant, the officer breached the accused's privacy interests and effected a "seizure" within the meaning of s. 8 of the *Charter*. At p. 435, La Forest J. stated:

> If I were to draw the line between a seizure and a mere finding of evidence, I would draw it logically and purposefully at the point at which it can reasonably be said that the individual had ceased to have a privacy interest in the subject-matter allegedly seized.

[76] Therefore, 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 of the appellant. Police are not relieved from the stringent standard of obtaining judicial authorization to conduct a search or seizure based on reasonable and probable grounds, simply because they are provided with evidence in circumstances where the accused's *Charter* rights were either not engaged or were not infringed in the initial gathering of that evidence: see e.g. *R. v. Law*, [2002] 1 S.C.R. 227, a case in which the police had lawfully recovered a stolen opened safe, wherein the Supreme Court held that the owner of the safe did not lose his expectation of privacy in the contents of the safe.

[77] This reasoning clearly applies to the laptop. The appellant's privacy interest with respect to his laptop continued throughout its transfer to police, notwithstanding that it was the property of the school board, and already lawfully seized by them. Personal information was also stored on the laptop. The police conducted a search and seizure of the laptop and seized the mirror image of the hard drive, capturing every piece of

personal information the appellant may have stored on it, including the photographs of his wife, without a warrant.

[78] The appellant also had a privacy interest in his personal internet browsing history and what it revealed about his personal predilections and choices. In *R. v. Morelli*, [2010] 1 S.C.R. 253, at para. 3, the Supreme Court referred to this as "the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet". Because the appellant had a continuing privacy interest in this information, the transfer of the disc with the temporary internet files to the police was a "seizure" within the meaning of s. 8 of the *Charter*.

[79] The police search of the laptop and the disc with the temporary internet files is therefore *prima facie* unreasonable. The onus shifts to the Crown to establish that this warrantless search by police was nonetheless reasonable. There were no exigent circumstances. Both the school environment and the evidence were secure; the teacher was suspended and the police were in possession of the discs and the laptop. The school board had no authority to consent to the search. This warrantless search was not reasonable. Therefore, the police violated the appellant's s. 8 rights when they searched the laptop and the disc with the temporary internet files.

[80] However, different considerations apply to the disc with the screen shot and the images of the student. Given that the photographs were taken from the school's network, using the school's computer and were the subject of the privacy interest of a student, the

appellant had no personal privacy interest in the data. The photographs were found by the technician in plain view, while engaged in permissible access. They were lawfully seized by the principal and transferred to police. As the functional equivalent of photographs in an envelope, the police did not need to conduct a further search of this evidence. Because the appellant had no privacy interest in the photographs themselves (as opposed to the presence of those photographs in the laptop), the delivery of the disc to police was not a seizure. This transfer is analogous to the transfer of the drugs found in the student's pocket by the vice-principal in *M.R.M*. In that case, the police did not require a search warrant to open the baggie and retrieve the drugs. Thus, the viewing of the photographs and the screen shot on the disc by police in this case was not a search or seizure within the meaning of s. 8 of the *Charter* and that evidence should not have been excluded by the trial judge.

4. Did the trial judge err in excluding the evidence of the laptop and the disc containing the temporary internet files?

[81] The trial judge applied the *Collins* test and determined that the evidence should be excluded under s. 24(2) of the *Charter*. He found that the police's warrantless seizure of the material, based on what little information was provided by school officials, was a serious breach of s. 8. He also held that the exclusion of the evidence that was unconstitutionally obtained would not bring the administration of justice into disrepute. Even if the nude images constituted child pornography (which the trial judge doubted), it

would be at the bottom end of material of that nature, since there was no commercial or exploitative aspect to the production of the photographs. There was no urgency and the failure to obtain a warrant "constituted an egregious breach of [the appellant's] section 8 Charter rights, this in an age when information is often more valuable than the hardware it is stored in and this in an age when personal privacy is so tied up with internet communications and computer technology."

[82] At the time of this pre-trial application, the Supreme Court had not yet released its decision in *R. v. Grant*, [2009] 2 S.C.R. 353, which modified the s. 24(2) analysis. In *Grant*, the Supreme Court of Canada clarified at para. 71 the criteria relevant to determining when "having regard to all the circumstances", admission of evidence obtained by a *Charter* breach "would bring the administration of justice into disrepute" and would thus require the evidence to be excluded under section 24(2):

> When faced with an application for exclusion under s. 24(2), a court must assess and balance the effect of admitting the evidence on society's confidence in the justice system having regard to: (1) the seriousness of the *Charter*-infringing state conduct (admission may send the message the justice system condones serious state misconduct), (2) the impact of the breach on the *Charter*-protected interests of the accused (admission may send the message that individual rights count for little), and (3) society's interest in the adjudication of the case on its merits.

[83] The court's role on a s. 24(2) application is to balance the assessments under each of these lines of inquiry. No overarching rule governs how the balance is to be struck.

a) The laptop and the mirror image of its hard drive

[84] The search and seizure of the laptop was not an inadvertent or minor violation of the appellant's privacy interests. However, there is no evidence that the police set out to deliberately disregard the appellant's right to privacy in the laptop. The officer believed that he did not need to get a warrant because the laptop was the property of the school board. While the officer's knowledge of the surrounding circumstances, including the fact that teachers used the computers for personal use, should have given rise to a consideration of whether the appellant had some expectation of privacy in the laptop, 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. However, given long established principles that ownership of property is not determinative, the seriousness of the violation, in these circumstances, weighs in favour of exclusion rather than admission of the evidence.

[85] With respect to the impact of the breach on the appellant's interests, the nature of the search was highly intrusive. The search actually conducted by the police was of the entire computer hard drive without any limitation in scope or method. In *Morelli*, Fish J. indicated for the majority of the Supreme Court of Canada:

> [2] It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.

> [3] First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet – generally by design, but sometimes by accident.

[86] While the present case does not involve the seizure of the appellant's personal computer from his home, it is nonetheless a computer which he was permitted by his employer to use for personal use. The appellant had expressly requested that there be no access to the photographs of his wife. The police search in this case would reveal all personal use of the computer without any prior judicial authorization. Thus, this intrusion into the informational privacy of the appellant was significant. Searching a computer that is used for personal purposes is potentially among the most invasive of searches.

[87] Finally, with respect to society's interest in the adjudication of this matter on the merits, the exclusion of the computer evidence does not "gut the prosecution" given the availability of other admissible evidence that establishes the photographs and where they were found. The copy of the images on the disc, made by the technician at the direction of the principal, is admissible. In these circumstances, I am not satisfied that exclusion of this evidence would exact too great a toll on the truth-seeking goal of this criminal trial. Such an invasive search, conducted without prior judicial authorization, cannot be

justified by the mere possibility that as the trial unfolds there may be further information in the appellant's hard drive that would become relevant and helpful to establishing the truth.

[88] I agree with the trial judge that the laptop and the mirror image of its hard drive should be excluded from the evidence in this trial pursuant to s. 24(2) of the *Charter*.

b) The disc containing the temporary internet files

[89] With respect to the disc containing the temporary internet files obtained from the appellant's internet browsing data, for reasons similar to those with respect to the laptop computer, the *Charter* violation is more than inadvertent or minor, but not as high as reckless or flagrant.

[90] With respect to the impact of this breach on the appellant's privacy interests, the temporary internet files reflect the sites the appellant visited on the internet using the computer. While the seizure was not profoundly intrusive or demeaning of the appellant's dignity, such information can disclose personal preferences and interests, as well as freedoms of thought and association, which the appellant would have a high expectation would remain private. As noted in *Morelli* at para. 105, computers can "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet." The fact that this kind of information is often readily recoverable from a computer does not

diminish our expectation of privacy about our actions in surfing the internet. The impact of this breach would tend to weigh in favour of exclusion of the evidence.

[91] With respect to society's interest in the adjudication on the merits, the potential use of the temporary internet files in the trial of the appellant was not clear, although 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. In the absence of a better understanding of the nature of this evidence, it is quite difficult to say that its exclusion would undermine the fact-finding process or exact too great a toll on the truth-seeking function of the appellant's trial. It is very unlikely that the exclusion of this evidence could be seen to "gut the prosecution".

[92] Weighing all these factors, the disc with the temporary internet files copied from the appellant's laptop computer and seized by police in violation of s. 8 of the *Charter* should be excluded. However, 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.

Conclusion

[93] In conclusion, the appellant's s. 8 *Charter* rights were not engaged as a result of the search by the technician and were not breached as a result of the searches and seizures conducted by the principal and the school board.

[94] The compact disc containing the photographs was not seized by the police in violation of s.8 and should not have been excluded by the trial judge. However, the warrantless police search and seizure of the laptop and the disc containing the temporary internet files breached the appellant's privacy rights under s. 8 of the *Charter*. I agree with the trial judge that the resulting evidence should be excluded under s. 24(2).

[95] Accordingly, I would grant leave to appeal and allow the appeal. I would set aside the decision of the summary conviction appeal judge, substitute an order excluding the evidence of the disc containing the temporary internet files and the laptop computer and its mirror image, and remit the matter back to the Ontario Court of Justice for trial.

RELEASED: March 22, 2011 "WKW"

"Karakatsanis J.A."

"I agree W. Winkler C.J.O."

"I agree Robert J. Sharpe J.A."