SUPREME COURT OF CANADA

CITATION: R. *v.* Cole, 2012 SCC 53, [2012] 3 S.C.R. 34

DATE: 20121019
DOCKET: 34268

BETWEEN:

Her Majesty The Queen
Appellant
and
Richard Cole
Respondent
- and -
Director of Public Prosecutions, Attorney General of Quebec, Criminal Lawyers' Association (Ontario), Canadian Civil Liberties Association
and
Canadian Association of Counsel to Employers
Interveners

CORAM: McLachlin C.J. and LeBel, Fish, Abella, Rothstein, Cromwell and Moldaver JJ.

REASONS FOR JUDGMENT: (paras. 1 to 106) — Fish J. (McLachlin C.J. and LeBel, Rothstein, Cromwell and Moldaver JJ. concurring)

DISSENTING REASONS: (paras. 107 to 136) — Abella J.

R. *v*. Cole, 2012 SCC 53, [2012] 3 S.C.R. 34

Her Majesty The Queen *Appellant*

v.

Richard Cole *Respondent*

and

Director of Public Prosecutions,
Attorney General of Quebec,
Criminal Lawyers' Association (Ontario),
Canadian Civil Liberties Association and
Canadian Association of Counsel to Employers *Interveners*

Indexed as: R. *v.* Cole

2012 SCC 53

File No.: 34268.

2012: May 15; 2012: October 19.

Present: McLachlin C.J. and LeBel, Fish, Abella, Rothstein, Cromwell and Moldaver JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO

Constitutional law — Charter of Rights — Search and seizure — Information contained on computer — Pornographic pictures of child found on employer-issued work computer — Whether accused had reasonable expectation of privacy in employer-issued work computer — Whether warrantless search and seizure of laptop computer and disc containing Internet files breached accused's rights under s. 8 of Charter — If so, whether evidence ought to be excluded pursuant to s. 24(2) of Charter.

The accused, a high-school teacher, was charged with possession of child pornography and unauthorized use of a computer. He was permitted to use his work-issued laptop computer for incidental personal purposes which he did. While performing maintenance activities, a technician found on the accused's laptop a hidden folder containing nude and partially nude photographs of an underage female student. The technician notified the principal, and copied the photographs to a compact disc. The principal seized the laptop, and school board technicians copied the temporary Internet files onto a second disc. The laptop and both discs were handed over to the police, who without a warrant reviewed their contents and then created a mirror image of the hard drive for forensic purposes. The trial judge excluded all of the computer material pursuant to ss. 8 and 24(2) of the *Canadian Charter of Rights and Freedoms*. The summary conviction appeal court reversed the decision, finding that there was no s. 8 breach. The Court of Appeal for Ontario set aside that decision and excluded the disc containing the temporary Internet files, the laptop and the mirror image of its hard drive. The disc containing the photographs of

the student was found to be legally obtained and therefore admissible. As the trial judge had wrongly excluded this evidence, the Court of Appeal ordered a new trial.

Held (Abella J. dissenting): The appeal should be allowed. The exclusionary order of the Court of Appeal is set aside and the order of a new trial is affirmed.

Per McLachlin C.J., and LeBel, Fish, Rothstein, Cromwell and Moldaver JJ.: Computers that are reasonably used for personal purposes — whether found in the workplace or the home — contain information that is meaningful, intimate, and touching on the user's biographical core. Canadians may therefore reasonably expect privacy in the information contained on these computers, at least where personal use is permitted or reasonably expected. Ownership of property is a relevant consideration, but is not determinative. Workplace policies are also not determinative of a person's reasonable expectation of privacy. Whatever the policies state, one must consider the totality of the circumstances in order to determine whether privacy is a reasonable expectation in the particular situation. While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely. A reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s. 8 of the *Charter*. Accordingly, it is subject to state intrusion only under the authority of a reasonable law.

The police in this case infringed the accused's rights under s. 8 of the *Charter*. The accused's personal use of his work-issued laptop generated information that is meaningful, intimate, and organically connected to his biographical core. Pulling in the other direction are the ownership of the laptop by the school board, the workplace policies and practices, and the technology in place at the school. These considerations diminished the accused's privacy interest in his laptop, at least in comparison to a personal computer, but they did not eliminate it entirely. On balance, the totality of the circumstances support the objective reasonableness of the accused's subjective expectation of privacy. While the principal had a statutory duty to maintain a safe school environment, and, by necessary implication, a reasonable power to seize and search a school-board issued laptop, the lawful authority of the accused's employer to seize and search the laptop did not furnish the police with the same power. Furthermore, a third party cannot validly consent to a search or otherwise waive a constitutional protection on behalf of another. The school board was legally entitled to inform the police of its discovery of contraband on the laptop. This would doubtless have permitted the police to obtain a warrant to search the computer for the contraband. But receipt of the computer from the school board did not afford the police warrantless access to the personal information contained within it. This information remained subject, at all relevant times, to the accused's reasonable and subsisting expectation of privacy.

Unconstitutionally obtained evidence should be excluded under s. 24(2) if, considering all of the circumstances, its admission would bring the administration

of justice into disrepute. The conduct of the police officer in this case was not an egregious breach of the *Charter*. While the police officer did attach great importance to the school board's ownership of the laptop, he did not do so to the exclusion of other considerations. The officer sincerely, though erroneously, considered the accused's *Charter* interests. Further, the officer had reasonable and probable grounds to obtain a warrant. Had he complied with the applicable constitutional requirements, the evidence would necessarily have been discovered. Finally, the evidence is highly reliable and probative physical evidence. The exclusion of the material would have a marked negative impact on the truth-seeking function of the criminal trial process. The admission of the evidence would not bring the administration of justice into disrepute and therefore the evidence should not be excluded.

Generally speaking, the decision to exclude evidence under s. 24(2) should be final. In very limited circumstances however, a material change of circumstances may justify a trial judge to revisit an exclusionary order. In this case, the Court of Appeal invited the trial judge to re-assess the admissibility of the temporary Internet files disc if the evidence becomes important to the truth-seeking function as the trial unfolds. Unconstitutionally obtained evidence, once excluded, will not become admissible simply because the Crown cannot otherwise satisfy its burden to prove the guilt of the accused beyond a reasonable doubt.

Per Abella J. (dissenting): While it is agreed that there has been a *Charter* breach, the evidence in this case should be excluded under s. 24(2). The

Charter-infringing conduct in this case was serious in its disregard for central and well-established *Charter* standards. The police officer had years of experience in investigating cyber-crime and was expected to follow established *Charter* jurisprudence. Further, the police officer's exclusive reliance on ownership to determine whether a warrant was required, was unreasonable and contradicted a finding of good faith for the purposes of s. 24(2). There were also no exigent circumstances or other legitimate reasons preventing the police from getting a warrant. The decision not to get a warrant mandates in favour of exclusion.

The impact of the breach on the accused's *Charter*-protected interests, even assuming that his reasonable expectation of privacy was reduced because it was a workplace computer, was significant given the extent of the intrusion into his privacy. The warrantless search and seizure in this case included the entire contents of the accused's computer. It had no restrictions as to scope. The extent of the search of the accused's hard drive and browsing history was significant and weighs in favour of exclusion.

Finally, while the evidence in this case is reliable, its importance to the prosecution's case is at best speculative given that the pornographic photographs themselves were admitted.

Balancing these factors, and in light of the deference owed to trial judges in applying s. 24(2), the evidence should be excluded.

Cases Cited

By Fish J.

Applied: *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; **referred to:** *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432; *R. v. Evans*, [1996] 1 S.C.R. 8; *R. v. Borden*, [1994] 3 S.C.R. 145; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579; *R. v. Nolet*, 2010 SCC 24, [2010] 1 S.C.R. 851; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393; *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631; *O'Connor v. Ortega*, 480 U.S. 709 (1987); *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211; *R. v. Colarusso*, [1994] 1 S.C.R. 20; *Quebec (Attorney General) v. Laroche*, 2002 SCC 72, [2002] 3 S.C.R. 708; *R. v. Jarvis*, 2002 SCC 73, [2002] 3 S.C.R. 757; *R. v. D'Amour* (2002), 166 C.C.C. (3d) 477; *R. v. Dyment*, [1988] 2 S.C.R. 417; *United States v. Matlock*, 415 U.S. 164 (1974); *Illinois v. Rodriguez*, 497 U.S. 177 (1990); *United States v. Ziegler*, 474 F.3d 1184 (2007); *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215; *R. v. Belnavis*, [1997] 3 S.C.R. 341; *R. v. Harrison*, 2009 SCC 34, [2009] 2 S.C.R. 494; *R. v. Calder*, [1996] 1 S.C.R. 660; *R. v. Underwood*, [1998] 1 S.C.R. 77; *R. v. M. (C.A.)*, [1996] 1 S.C.R. 500; *R. v. Trask*, [1987] 2 S.C.R. 304.

By Abella J. (dissenting)

R. v. Morelli, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Kokesch*, [1990] 3 S.C.R. 3; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Wong*, [1990] 3 S.C.R. 36; *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631; *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; *R. v. Harrison*, 2009 SCC 34, [2009] 2 S.C.R. 494.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).
Criminal Code, R.S.C. 1985, c. C-46, ss. 163.1(4), 342.1(1).
Education Act, R.S.O. 1990, c. E.2, s. 265.

Authors Cited

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1970.

APPEAL from a judgment of the Ontario Court of Appeal (Winkler C.J.O. and Sharpe and Karakatsanis JJ.A.), 2011 ONCA 218, 105 O.R. (3d) 253, 277 O.A.C. 50, 231 C.R.R. (2d) 76, 269 C.C.C. (3d) 402, 83 C.R. (6th) 1, 2011 CLLC ¶210-018, 90 C.C.E.L. (3d) 1, [2011] O.J. No. 1213 (QL), 2011 CarswellOnt 1766, setting aside a decision of Kane J. (2009), 190 C.R.R. (2d) 130, 2009 CanLII 20699, [2009] O.J. No. 1755 (QL), 2009 CarswellOnt 2251, setting aside a decision of

Guay J., 2008 ONCJ 278, 175 C.R.R. (2d) 263, [2008] O.J. No. 2417 (QL), 2008 CarswellOnt 3601. Appeal allowed, Abella J. dissenting.

Amy Alyea and *Frank Au*, for the appellant.

Frank Addario, *Gerald Chan* and *Nader R. Hasan*, for the respondent.

Ronald C. Reimer and *Monique Dion*, for the intervener the Director of Public Prosecutions.

Dominique A. Jobin and *Gilles Laporte*, for the intervener the Attorney General of Quebec.

Jonathan Dawe and *Michael Dineen*, for the intervener the Criminal Lawyers' Association (Ontario).

Jonathan C. Lisus and *Michael Perlin*, for the intervener the Canadian Civil Liberties Association.

Daniel Michaluk and *Joseph Cohen-Lyons*, for the intervener the Canadian Association of Counsel to Employers.

The judgment of McLachlin C.J. and LeBel, Fish, Rothstein, Cromwell and Moldaver JJ. was delivered by

FISH J. —

I

[1] The Court left no doubt in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, that Canadians may reasonably expect privacy in the information contained on their own *personal* computers. In my view, the same applies to information on *work* computers, at least where personal use is permitted or reasonably expected.

[2] Computers that are reasonably used for personal purposes — whether found in the workplace or the home — contain information that is meaningful, intimate, and touching on the user's biographical core. *Vis-à-vis* the state, everyone in Canada is constitutionally entitled to expect privacy in personal information of this kind.

[3] While workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the expectation entirely: The nature of the information at stake exposes the likes, interests, thoughts, activities, ideas, and searches for information of the individual user.

[4] Such was the case here. Mr. Cole, a high-school teacher, was permitted to use his work-issued laptop computer for incidental personal purposes. He did. He browsed the Internet and stored personal information on his hard drive.

[5] While performing maintenance activities, a technician found on Mr. Cole's laptop a hidden folder containing nude and partially nude photographs of a female student. He notified the principal, and, under the latter's discretion, copied the photographs to a compact disc or CD. The principal seized the laptop, and school board technicians copied the temporary Internet files onto a second CD. The laptop and both CDs were handed over to the police, who without a warrant reviewed their contents and then created a mirror image of the hard drive for forensic purposes.

[6] Mr. Cole 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*, R.S.C. 1985, c. C-46, respectively, and prosecuted by way of summary conviction. The trial judge excluded all of the computer material pursuant to ss. 8 and 24(2) of the *Canadian Charter of Rights and Freedoms*. The Crown offered no further evidence and the charges were therefore dismissed (2008 ONCJ 278, 175 C.R.R. (2d) 263).

[7] The summary conviction appeal court reversed the decision of the trial judge, finding that there was no s. 8 breach ((2009), 190 C.R.R. (2d) 130). The Court of Appeal for Ontario set aside that decision and excluded the disc containing the

temporary Internet files, the laptop, and the mirror image of its hard drive (2011 ONCA 218, 105 O.R. (3d) 253).

[8] I agree with the Court of Appeal that the police infringed Mr. Cole's rights under s. 8 of the *Charter*. He expected a measure of privacy in his personal information on the laptop. Even taking into account the relevant workplace policies, this expectation of privacy was reasonable in the circumstances. It was, however, a *diminished expectation of privacy* in comparison with the privacy interest considered in *Morelli* — which, unlike this case, involved a personal computer that belonged to Mr. Morelli and was searched and seized in his home.

[9] A reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy, protected by s. 8 of the *Charter*. Accordingly, it is subject to state intrusion only under the authority of a reasonable law.

[10] The Crown in this case could point to no law authorizing the police to conduct, as they did, a warrantless search of Mr. Cole's work laptop. The lawful authority of his *employer* — a school board — to seize and search the laptop did not furnish the *police* with the same power. And the school board's "third party consent" to the search was of no legal consequence.

[11] Unlike the Court of Appeal, however, I would not exclude any of the unconstitutionally obtained evidence under s. 24(2).

[12] For these reasons and the reasons that follow, I would allow the appeal and set aside the decision of the Court of Appeal.

II

[13] The parties agree that Mr. Cole may face a new trial regardless of the outcome of this appeal: If the appeal is allowed, the Crown may proceed to a new trial with the benefit of all of the computer evidence excluded by the trial judge; if the Crown's appeal is dismissed, the Crown can still return to trial, but only with regard to the disc containing the nude photographs.

[14] As a new trial may thus be had, I shall discuss the facts only to the extent necessary to explain my conclusion.

[15] Mr. Cole, as mentioned earlier, was a high-school teacher. In addition to his regular teaching duties, he was responsible for policing the use by students of their networked laptops. To this end, he was supplied with a laptop owned by the school board and accorded domain administration rights on the school's network. This permitted him to access the hard drives of the students' laptops.

[16] The use of Mr. Cole's work-issued laptop was governed by the school board's Policy and Procedures Manual, which allowed for incidental personal use of the board's information technology. The policy stipulated that teachers' e-mail correspondence remained private, but subject to access by school administrators if

specified conditions were met. It did not address privacy in other types of files, but it did state that "all data and messages generated on or handled by board equipment are considered to be the property of [the school board]".

[17] There is evidence as well that the school's Acceptable Use Policy — written for and signed by students — applied *mutatis mutandis* to teachers. This policy not only restricted the uses to which the students could put their laptops, but also warned users not to expect privacy in their files.

[18] Mr. Cole was not the only person who could remotely access networked laptops. School board technicians could do so as well. While performing maintenance activities, a school board technician found, on Mr. Cole's laptop, a hidden folder containing nude and partially nude photographs of an underage female student.

[19] As mentioned earlier, the technician notified the principal, who directed him to copy the photographs to a compact disc. After discussing the matter with school board officials, the principal seized the laptop.

[20] At no time did Mr. Cole disclose his password. But he did ask the principal not to access a folder containing photographs of his wife.

[21] Technicians at the school board eventually gained access to Mr. Cole's laptop and made a compact disc containing his temporary Internet files, which is said by the Crown to contain pornographic images.

[22] The next day, a police officer attended at the school and at the offices of the school board, where he took possession of the laptop and the two CDs: one containing photographs of the student; the other, Mr. Cole's temporary Internet files. The officer reviewed the contents of both discs at the police station, and then sent the laptop away for forensic examination. A mirror image of the hard drive was created for that purpose.

[23] At no time did the officer obtain a warrant to search the laptop's hard drive or either of the compact discs.

III

[24] Mr. Cole brought a pre-trial motion seeking exclusion of the computer evidence pursuant to s. 24(2) of the *Charter*. The trial judge found that the police had violated Mr. Cole's s. 8 *Charter* rights, and, for that reason, he excluded all of the computer evidence. The summary conviction appeal court granted the Crown's appeal, finding that Mr. Cole had no reasonable expectation of privacy in his work laptop.

[25] Mr. Cole appealed successfully to the Court of Appeal for Ontario. The Court of Appeal held that Mr. Cole had a reasonable expectation of privacy in the informational content of the laptop, but that this expectation was "modified to the extent that [Mr. Cole] 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" (para. 47).

[26] On this approach, the initial remote access by the technician was not a "search" for the purposes of s. 8. But the examinations by the police, the principal, and the school board (assuming the *Charter* applied to the latter two) *did* engage s. 8.

[27] The Court of Appeal concluded that the search and seizure of the laptop by the principal and the school board was authorized by law and reasonable. The disc containing the photographs was thus created without breaching s. 8. And since Mr. Cole had no privacy interest in the photographs themselves, he had no legal basis to attack the search and seizure by the police of the disc to which they had been copied.

[28] The laptop and the disc with Mr. Cole's temporary Internet files, however, involve different considerations. Mr. Cole had a continuing reasonable expectation of privacy in this material, and its seizure by school officials did not endow the police with *their* authority. Nor could the school board consent to the search by the police. As the police had no other lawful authority, the s. 8 breach was established.

[29] The Court of Appeal excluded the laptop and the mirror image of its hard drive pursuant to s. 24(2) of the *Charter*. The court also excluded the disc containing the Internet files, but only provisionally, leaving it "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" (para. 92).

[30] The disc containing the photographs of the student was legally obtained and therefore admissible. As the trial judge had wrongly excluded this evidence, the Court of Appeal ordered a new trial.

[31] The Crown appeals from the order excluding the laptop, its mirror image, and the Internet files disc. Mr. Cole does not challenge the admission, under ss. 8 and 24(2) of the *Charter*, of the disc containing the photographs, or the order of a new trial.

[32] This appeal thus raises three issues: (1) whether the Court of Appeal erred in concluding that Mr. Cole had a reasonable expectation of privacy in his employer-issued work computer; (2) whether the Court of Appeal erred in concluding that the search and seizure by the police of the laptop and the disc containing the Internet files was unreasonable within the meaning of s. 8 of the *Charter*; and (3) whether the Court of Appeal erred in excluding the evidence under s. 24(2) of the *Charter*.

[33] I would answer the first two questions in the negative, but not the third.

IV

[34] Section 8 of the *Charter* guarantees the right of everyone in Canada to be secure against unreasonable search or seizure. An inspection is a search, and a taking is a seizure, where a person has a reasonable privacy interest in the object or subject matter of the state action and the information to which it gives access (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 18; *R. v. Evans*, [1996] 1 S.C.R. 8, at para. 11; *R. v. Borden*, [1994] 3 S.C.R. 145, at p. 160).

[35] Privacy is a matter of reasonable expectations. An expectation of privacy will attract *Charter* protection if reasonable and informed people in the position of the accused would expect privacy (*R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at paras. 14-15).

[36] If the claimant has a reasonable expectation of privacy, s. 8 is engaged, and the court must then determine whether the search or seizure was reasonable.

[37] Where, as here, a search is carried out without a warrant, it is presumptively unreasonable (*R. v. Nolet*, 2010 SCC 24, [2010] 1 S.C.R. 851, at para. 21; *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 161). To establish reasonableness, the Crown must prove on the balance of probabilities (1) that the search was authorized by law, (2) that the authorizing law was itself reasonable, and (3) that the authority to conduct the search was exercised in a reasonable manner (*Nolet*, at para. 21; *R. v. Collins*, [1987] 1 S.C.R. 265, at p. 278).

[38] Before applying this analytical framework here, I pause to explain why it is unnecessary on this appeal to decide whether the *Charter* applies to school officials. The Crown conceded in the courts below that it does. Like the Court of Appeal, I shall proceed on that assumption, as did Cory J. in *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at paras. 24-25.

V

[39] Whether Mr. Cole had a reasonable expectation of privacy depends on the "totality of the circumstances" (*R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 45).

[40] The "totality of the circumstances" test is one of substance, not of form. Four lines of inquiry guide the application of the test: (1) an examination of the subject matter of the alleged search; (2) a determination as to whether the claimant had a direct interest in the subject matter; (3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances (*Tessling*, at para. 32; *Patrick*, at para. 27). I will discuss each in turn.

[41] In this case, the subject matter of the alleged search is the data, or *informational content* of the laptop's hard drive, its mirror image, and the Internet files disc — not the devices themselves.

[42] Our concern is thus with *informational privacy*: "[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (*Tessling*, at para. 23, quoting A. F. Westin, *Privacy and Freedom* (1970), at p. 7).

[43] Mr. Cole's direct interest and subjective expectation of privacy in the informational content of his computer can readily be inferred from his use of the laptop to browse the Internet and to store personal information on the hard drive.

[44] The remaining question is whether Mr. Cole's subjective expectation of privacy was objectively reasonable.

[45] There is no definitive list of factors that must be considered in answering this question, though some guidance may be derived from the relevant case law. As Sopinka J. explained in *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.

[46] The closer the subject matter of the alleged search lies to the biographical core of personal information, the more this factor will favour a reasonable expectation of privacy. Put another way, the more personal and confidential the information, the

more willing reasonable and informed Canadians will be to recognize the existence of a constitutionally protected privacy interest.

[47] Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (*Morelli*, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "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" (*ibid*.).

[48] This sort of private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter*.

[49] Like *Morelli*, this case involves highly revealing and meaningful information about an individual's personal life — a factor strongly indicative of a reasonable expectation of privacy. Unlike in *Morelli*, however, this case involves a *work-issued* laptop and not a personal computer found in a private residence.

[50] The Policy and Procedures Manual of the school board asserted ownership over not only the hardware, but also the data stored on it: "Information technology systems and all data and messages generated on or handled by board equipment are considered to be the property of [the board], and are not the property of users of the information technology".

[51] While the ownership of property is a relevant consideration, it is not determinative (*R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631, at para. 22). Nor should it carry undue weight within the contextual analysis. As Dickson J. (later C.J.) noted in *Hunter*, at p. 158, there is "nothing in the language of [s. 8] to restrict it to the protection of property or to associate it with the law of trespass".

[52] The *context* in which personal information is placed on an employer-owned computer is nonetheless significant. The policies, practices, and customs of the workplace are relevant to the extent that they concern the use of computers by employees. These "operational realities" may diminish the expectation of privacy that reasonable employees might otherwise have in their personal information (*O'Connor v. Ortega*, 480 U.S. 709 (1987), at p. 717, *per* O'Connor J.).

[53] Even as modified by practice, however, written policies are not determinative of a person's reasonable expectation of privacy. Whatever the policies state, one must consider the *totality* of the circumstances in order to determine whether privacy is a reasonable expectation in the particular situation (*R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, *per* Deschamps J.).

[54] In this case, the operational realities of Mr. Cole's workplace weigh both for and against the existence of a reasonable expectation of privacy. *For*, because written policy and actual practice permitted Mr. Cole to use his work-issued laptop for personal purposes. *Against*, because both policy and technological reality

deprived him of exclusive control over — and access to — the personal information he chose to record on it.

[55] As mentioned earlier, the Policy and Procedures Manual stated that the school board owned "all data and messages generated on or handled by board equipment". Moreover, the principal reminded teachers, annually, that the Acceptable Use Policy applied to them. This policy provided that "[t]eachers and administrators may monitor all student work and e-mail including material saved on laptop hard drives", and warned that "[u]sers should NOT assume that files stored on network servers or hard drives of individual computers will be private".

[56] Though Mr. Cole's laptop was equipped with a password, the contents of his hard drive were thus available to all other users and technicians with domain administration rights — at least when the computer was connected to the network. And even if the Acceptable Use Policy did not directly apply to teachers, as Mr. Cole maintains, he and other teachers were in fact put on notice that the privacy they might otherwise have expected in their files was limited by the operational realities of their workplace.

[57] The "totality of the circumstances" consists of many strands, and they pull in competing directions in this case. On balance, however, they support the objective reasonableness of Mr. Cole's subjective expectation of privacy.

[58] The nature of the information in issue heavily favours recognition of a constitutionally protected privacy interest. Mr. Cole's personal use of his work-issued laptop generated information that is meaningful, intimate, and organically connected to his biographical core. Pulling in the other direction, of course, are the ownership of the laptop by the school board, the workplace policies and practices, and the technology in place at the school. These considerations diminished Mr. Cole's privacy interest in his laptop, at least in comparison to the personal computer at issue in *Morelli*, but they did not eliminate it entirely.

VI

[59] As Mr. Cole had a reasonable expectation of privacy in his Internet browsing history and the informational content of his work-issued laptop, any non-consensual examination by the state was a "search"; and any taking, a "seizure".

[60] Mr. Cole does not challenge the initial inspection of the laptop by the school technician in the context of routine maintenance activities. He concedes, moreover, that the technician did not breach his s. 8 rights. In this light, I leave for another day the finer points of an employer's right to monitor computers issued to employees.

[61] The Court of Appeal concluded that, in the circumstances of this case, the subsequent search and seizure of the laptop by school officials acting under the

direction of the principal was not unreasonable within the meaning of s. 8 of the *Charter*. Mr. Cole does not challenge this conclusion.

[62] In any event, I agree with the Court of Appeal. The principal had a statutory duty to maintain a safe school environment (*Education Act*, R.S.O. 1990, c. E.2, s. 265), and, by necessary implication, a reasonable power to seize and search a school-board-issued laptop if the principal believed on reasonable grounds that the hard drive contained compromising photographs of a student. This implied power is not unlike the one found by the majority of this Court in *M. (M.R.)*, at para. 51.

[63] I likewise agree with the Court of Appeal that other school board officials had the same implied powers of search and seizure as the principal (paras. 64-66).

[64] I turn then to the conduct of the police.

[65] The police may well have been authorized to take physical control of the laptop and CD *temporarily, and for the limited purpose of safeguarding potential evidence of a crime until a search warrant could be obtained*. However, that is not what occurred here. Quite the contrary: The police seized the laptop and CD *in order to search their contents for evidence of a crime* without the consent of Mr. Cole, and without prior judicial authorization.

[66] The unresolved question on this appeal is whether the authority of the school officials afforded *the police* lawful authority to conduct this warrantless search and seizure. In my view, it did not.

[67] In taking possession of the computer material and examining its contents, the police acted independently of the school board (*R. v. Colarusso*, [1994] 1 S.C.R. 20, at pp. 58-60). The fact that the school board had acquired lawful possession of the laptop *for its own administrative purposes* did not vest in the police a delegated or derivative power to appropriate and search the computer *for the purposes of a criminal investigation*.

[68] This was made clear in *Colarusso*, where a coroner who had lawfully seized bodily samples then turned them over to the police. As La Forest J. explained:

> The arguments advanced by the Crown seeking to establish the reasonableness of warrantless seizures by a coroner rely on the underlying premise that the coroner fulfils an essential non-criminal role. The state cannot, however, have it both ways; it cannot be argued that the coroner's seizure is reasonable because it is independent of the criminal law enforcement arm of the state while the state is at the same time attempting to introduce into criminal proceedings the very evidence seized by the coroner. It follows logically, in my opinion, that a seizure by a coroner will only be reasonable while the evidence is used for the purpose for which it was seized, namely, for determining whether an inquest into the death of the individual is warranted. Once the evidence has been appropriated by the criminal law enforcement arm of the state for use in criminal proceedings, there is no foundation on which to argue that the coroner's seizure continues to be reasonable. [pp. 62-63]

[69] Where a lower constitutional standard is applicable in an administrative context, as in this case, the police cannot invoke that standard to evade the prior judicial authorization that is normally required for searches or seizures in the context of criminal investigations.

[70] The Crown relies on *Quebec (Attorney General) v. Laroche*, 2002 SCC 72, [2002] 3 S.C.R. 708, *R. v. Jarvis*, 2002 SCC 73, [2002] 3 S.C.R. 757, and *R. v. D'Amour* (2002), 166 C.C.C. (3d) 477 (Ont. C.A.), for the proposition that a warrant is not required for a regulatory authority to transfer material to law enforcement officers — and that this empowers the officers to examine the transferred materials without a warrant.

[71] I would reject this submission. All of the cases relied on by the Crown arose in heavily regulated environments. In each instance, given the regulated nature of the documents in question, the individual claiming the protection of s. 8 did not have a reasonable expectation of preventing or controlling the further dissemination of his or her information to the law enforcement branch of the state.

[72] No warrant was required because the claimants in the cases cited by the Crown, unlike Mr. Cole in this case, did not have a reasonable expectation of privacy in the information remitted to law enforcement officials. Mr. Cole, throughout, retained a reasonable and "*continuous*" expectation of privacy in the personal information on his work-issued laptop (*Buhay*, at para. 33 (emphasis added); *R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 435).

[73] The school board was, of course, legally entitled to inform the police of its discovery of contraband on the laptop. This would doubtless have permitted the police to obtain a warrant to search the computer for the contraband. But receipt of the computer from the school board did not afford the police *warrantless access* to the personal information contained within it. This information remained subject, at all relevant times, to Mr. Cole's reasonable and *subsisting* expectation of privacy.

[74] The Crown alleges a second justification for the conduct of the police: third party consent. An employer (a third party), says the Crown, can validly consent to a warrantless search or seizure of a laptop issued to one of its employees. The underlying premise of this submission is that a third party may waive another person's privacy interest — thereby disengaging that person's guarantee under s. 8 of the *Charter*.

[75] In the United States, unlike in Canada, there is high authority for a doctrine of third party consent (*United States v. Matlock*, 415 U.S. 164 (1974); *Illinois v. Rodriguez*, 497 U.S. 177 (1990)).

[76] *Matlock* is premised on the notion that third party consent is justifiable because the individual voluntarily assumed the risk that his information would fall into the hands of law enforcement (see *United States v. Ziegler*, 474 F.3d 1184 (9th Circ. 2007), at p. 1191). However, this Court rejected that sort of "risk analysis" in *R. v. Duarte*, [1990] 1 S.C.R. 30, at pp. 47-48, and *R. v. Wong*, [1990] 3 S.C.R. 36, at p. 45.

[77] Moreover, the doctrine of third party consent is inconsistent with this Court's jurisprudence on *first party* consent. As Iacobucci J. explained in *Borden*, at p. 162, "[i]n order for a waiver of the right to be secure against an unreasonable seizure to be effective, the person purporting to consent must be possessed of the requisite informational foundation for a true relinquishment of the right."

[78] For consent to be valid, it must be both voluntary and informed. The adoption of a doctrine of third party consent in this country would imply that the police could interfere with an individual's privacy interests on the basis of a consent that is *not* voluntarily given by the rights holder, and *not* necessarily based on sufficient information in his or her hands to make a meaningful choice.

[79] I would therefore reject the Crown's contention that a third party could validly consent to a search or otherwise waive a constitutional protection on behalf of another.

VII

[80] With the *Charter* breach established, the inquiry shifts to s. 24(2).

[81] Unconstitutionally obtained evidence should be excluded under s. 24(2) if, considering all of the circumstances, its admission would bring the administration of justice into disrepute. This determination requires a balancing assessment involving three broad inquiries: (1) the seriousness of the *Charter*-infringing state

conduct; (2) the impact of the breach on the *Charter*-protected interests of the accused; and (3) society's interest in the adjudication of the case on its merits (*R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353, at para. 71).

[82] The standard of review is deferential: "Where a trial judge has considered the proper factors and has not made any unreasonable finding, his or her determination is owed considerable deference on appellate review" (*R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215, at para. 44). But where the relevant factors have been overlooked or disregarded, a fresh *Grant* analysis is both necessary and appropriate.

[83] Both the trial judge and the Court of Appeal — erroneously, in my respectful view — excluded the unconstitutionally obtained evidence pursuant to s. 24(2) of the *Charter*.

[84] Regarding the seriousness of the *Charter*-infringing conduct, the courts below focused on the actions of Detective Constable Timothy Burtt, the officer who took possession of the computer material, who searched the discs, and who sent the laptop away for forensic examination. The trial judge concluded that this officer's actions were "egregious" (para. 26), and the Court of Appeal considered his conduct serious enough to favour exclusion.

[85] I am unable to share either conclusion.

[86] The police officer did not knowingly or deliberately disregard the warrant requirement. As events were unfolding in this case, the law governing privacy expectations in work computers was still unsettled. Without the guidance of appellate case law, D.C. Burtt believed, erroneously but understandably, that he had the power to search without a warrant.

[87] He did not act negligently or in bad faith. Nor does his conduct evidence insensitivity to *Charter* values, or an unacceptable ignorance of Mr. Cole's rights under the *Charter*. The officer did not rely exclusively, as the courts below suggested, on his mistaken belief that the ownership of the laptop was necessarily determinative. While this was an important factor underlying his decision not to obtain a search warrant, the officer also turned his mind to whether Mr. Cole had an expectation of privacy in the laptop (p. 130). He was alert to the possibility that the hard drive contained private or privileged material (pp. 130-31 and 164). And he testified that he intended to respect Mr. Cole's privacy interest in this regard (p. 131).

[88] More particularly, D.C. Burtt testified as follows:

> Q. Did you consider whether or not Richard Cole had any expectation of privacy in that computer?
>
> A. I did consider that. The information that I was receiving was that it was the School Board's computer and that was their property. I had never received any information in regards to Mr. Cole owning that computer *or that he had any privileged material*. And I've dealt with cases where there have been privileged material on a laptop or on a computer. And the only information I had received about any private material that was on that computer came from Mr. Bourget and that was in regards to some

> images of Mr. Cole's — personal images of his wife and that was *the only information I had in regards to any private information there*.
>
> Q. *And having received that information that there may be images of his wife on the laptop, would you respect that any privacy interest in those photographs?*
>
> A. *Yes, sir*. Business computer or any computers may have some personal stuff on there. [Emphasis added.]

[89] What of the fact that the officer had reasonable and probable grounds to obtain a warrant? In some circumstances, this may aggravate the seriousness of the breach (*Côté*, at para. 71). Where a police officer could have acted constitutionally but did not, this might indicate that the officer adopted a casual attitude toward — or, still worse, deliberately flouted — the individual's *Charter* rights (*Buhay*, at paras. 63-64). But that is not this case: The officer, as mentioned earlier, appears to have sincerely, though erroneously, considered Mr. Cole's *Charter* interests.

[90] Accordingly, in my view, the trial judge's finding of "egregious" conduct was tainted by clear and determinative error (*Côté*, at para. 51). On the undisputed evidence, the conduct of the officer was simply not an egregious breach of the *Charter*. As earlier seen, the officer did attach great importance to the school board's ownership of the laptop, but not to the exclusion of other considerations. He did not "confuse ownership of hardware with privacy in the contents of software" (trial reasons, at para. 29).

[91] Turning then to the impact of the breach on Mr. Cole's *Charter*-protected interests, the question relates to "the extent to which the breach actually undermined the interests protected by the right infringed" (*Grant*, at para. 76). In the context of a s. 8 breach, as here, the focus is on the magnitude or intensity of the individual's reasonable expectation of privacy, and on whether the search demeaned his or her dignity (*R. v. Belnavis*, [1997] 3 S.C.R. 341, at para. 40; *Grant*, at para. 78).

[92] In his s. 24(2) analysis, the trial judge neglected entirely to consider the diminished nature of Mr. Cole's reasonable expectation of privacy. Likewise, the Court of Appeal overlooked the fact that the operational realities of Mr. Cole's workplace attenuated the effect of the breach on his *Charter*-protected interests.

[93] Moreover, the courts below failed to consider the impact of the "discoverability" of the computer evidence on the second *Grant* inquiry. As earlier noted, the officer had reasonable and probable grounds to obtain a warrant. Had he complied with the applicable constitutional requirements, the evidence would necessarily have been discovered. This further attenuated the impact of the breach on Mr. Cole's *Charter*-protected interests (*Côté*, at para. 72).

[94] Finally, I turn to the third *Grant* inquiry: society's interest in an adjudication on the merits. The question is "whether the truth-seeking function of the criminal trial process would be better served by admission of the evidence, or by its exclusion" (*Grant*, at para. 79).

[95] Not unlike the considerations under the first and second inquiries, the considerations under this third inquiry must not be permitted to overwhelm the s. 24(2) analysis (*Côté*, at para. 48; *R. v. Harrison*, 2009 SCC 34, [2009] 2 S.C.R. 494, at para. 40). They are nonetheless entitled to appropriate weight and, in the circumstances of this case, they clearly weigh against exclusion of the evidence.

[96] The laptop, the mirror image of its hard drive, and the disc containing Mr. Cole's temporary Internet files are all highly reliable and probative physical evidence. And while excluding it would not "gut" the prosecution entirely, I accept the Crown's submission that the forensic examination of the laptop, at least, is "critical": the metadata on the laptop may allow the Crown to establish, for example, when the photographs were downloaded and whether they have ever been accessed.

[97] In sum, the admission of the evidence would not bring the administration of justice into disrepute. The breach was not high on the scale of seriousness, and its impact was attenuated by both the diminished privacy interest and the discoverability of the evidence. The exclusion of the material would, however, have a marked negative impact on the truth-seeking function of the criminal trial process.

[98] For all of these reasons, I would not exclude the evidence unlawfully obtained by the police in this case.

[99] Having concluded that none of the computer evidence should have been excluded pursuant to s. 24(2), it is not strictly necessary to address the provisional nature of the Court of Appeal's ruling in respect of the Internet files disc. Nevertheless, I find it appropriate to do so.

[100] Generally speaking, the decision to exclude evidence under s. 24(2) should be final. In "very limited circumstances", however, a "material change of circumstances" may justify a trial judge to revisit an exclusionary order (*R. v. Calder*, [1996] 1 S.C.R. 660, at para. 35).

[101] For reasons of principle and of practice, the exclusion of evidence should generally be final. As the intervener Criminal Lawyers' Association (Ontario) points out, an accused is entitled, as a matter of principle, to know the case to meet. If an exclusionary order is revisited after the Crown closes its case, this principle is necessarily undermined. If the case to meet continues to shift, the prejudice is obvious and the trial might well become unmanageable (*R. v. Underwood*, [1998] 1 S.C.R. 77, at paras. 6-7).

[102] Moreover, even when an exclusionary order is revisited *before* the Crown closes its case, there is a serious danger of prejudice to the defendant. The decisions of defence counsel over the course of the trial — premised on the assumption that the evidence has been excluded — risk being undercut. It would be extraordinarily difficult for a trial court to remedy this sort of prejudice.

[103] In this case, the Court of Appeal invited the trial judge "to re-assess the admissibility of [the temporary Internet files disc] if the evidence becomes important to the truth-seeking function as the trial unfolds" (para. 92).

[104] In my respectful view, this would not — at least not on its own — qualify as "very limited circumstances" justifying an exception to the rule. Unconstitutionally obtained evidence, once excluded, will not become admissible simply because the Crown cannot otherwise satisfy its burden to prove the guilt of the accused beyond a reasonable doubt.

IX

[105] As stated at the outset, I would allow the appeal, set aside the exclusionary order of the Court of Appeal, and affirm the order of a new trial.

[106] Mr. Cole asks that he be awarded his costs regardless of the outcome of the appeal. While the Court has the discretion to make such an order, I would decline to do so. There is nothing "remarkable" about this case — the principal criterion — and there was no allegation of "oppressive or improper conduct" on the part of the Crown (*R. v. Trask*, [1987] 2 S.C.R. 304, at p. 308; *R. v. M. (C.A.)*, [1996] 1 S.C.R. 500, at para. 97).

The following are the reasons delivered by

[107] ABELLA J. (dissenting) — While I agree with Justice Fish that there has been a *Charter* breach, in my respectful view, like Justice Karakatsanis in the Court of Appeal, I would exclude the disc containing the temporary Internet files and the copy of the hard drive.

[108] In *R. v. Morelli*, [2010] 1 S.C.R. 253, Fish J. observed that "it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer" (para. 105). Workplace computers, while clearly engaging different considerations, nonetheless attract many of the same privacy concerns as home computers.

[109] Workplace computers are increasingly given to employees for their exclusive use, and employees are allowed — and often expected — to use them away from the workplace for both work-related and personal use. And as more data is stored in the cloud and accessed on both workplace and personal computers, the ownership of the device or the data, far from being determinative of the reasonable expectation of privacy, becomes an increasingly unhelpful marker. In deciding whether to exclude evidence illegally seized from workplace computers, this blurring of the line between personal and workplace usage should inform the analysis.

[110] Three considerations come into play in this case in determining whether to exclude the evidence. The first is the seriousness of the *Charter*-infringing state

conduct, which looks at whether the police acted in good faith based on their presumed knowledge of the law. Detective Constable Burtt, an experienced officer with years of experience in investigating cyber-crime, was expected to follow established *Charter* jurisprudence. His failure to do so, in my view, represents a serious breach.

[111] This Court's decision in *R. v. Kokesch*, [1990] 3 S.C.R. 3, is particularly helpful. In that case, the Court decided that a perimeter search of the accused's residence violated s. 8 of the *Charter*. Prior to *Kokesch*, it was unclear whether such a search violated the *Charter*. Nonetheless, the Court excluded the impugned evidence, noting that the law of trespass *was* firmly settled, and that the police "ought to have known" that they were trespassing. In the words of Sopinka J.:

> I do not wish to be understood as imposing upon the police a burden of instant interpretation of court decisions. The question of the length of time after a judgment that ought to be permitted to pass before knowledge of its content is attributed to the police for the purposes of assessing good faith is an interesting one, but it does not arise on these facts. The police here had the benefit of slightly more than twelve years to study *Eccles*, slightly less than six years to consider *Colet*, and slightly more than two years to digest the constitutional warrant requirement set out in *Hunter*. Any doubt they may have had about their ability to trespass in the absence of specific statutory authority to do so was manifestly unreasonable, and cannot, as a matter of law, be relied upon as good faith for the purposes of s. 24(2). [Emphasis added; p. 33.]

[112] In other words, the Court concluded that if, in conducting their search, the police disregarded settled law, any specific uncertainty in the law becomes far less

determinative. Otherwise, it would open the door too widely for the admission of evidence under s. 24(2).

[113] In this case, the trial judge found that D.C. Burtt assumed that "because the laptop belonged to the Rainbow District School Board, there was no need for him to get a warrant". To borrow from *Kokesch*, D.C. Burtt's exclusive reliance on ownership to determine whether a warrant was required was unreasonable and cannot be relied on as good faith for the purposes of s. 24(2).

[114] While the law relating to the search of workplace computers was unsettled at the time of the search, what *was* settled was the fact that property rights did not determine whether a warrant was required. In 1984, *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, divorced the concept of privacy from the law of trespass and said that s. 8 protects "people, not places" (p. 159). In 1990, the Court found a reasonable expectation of privacy in a hotel room in *R. v. Wong*, [1990] 3 S.C.R. 36, and in 2003, found a reasonable expectation of privacy in a rented locker in *R. v. Buhay*, [2003] 1 S.C.R. 631. The search in this case, in June 2006, occurred many years after this established jurisprudence, undeniably a sufficient amount of time for an officer who had years of experience in cyber-crime to have known that property interests did not determine the reasonable expectation of privacy.

[115] Justice Fish finds that the trial judge made a "clear and determinative" error in finding that D.C. Burtt wrongly relied on the ownership of the laptop in

deciding not to get a warrant. With respect, in my view the trial judge's conclusion is fully supported by the evidence.

[116] D.C. Burtt accepted that he had reasonable grounds for a warrant. Then, on multiple occasions, he stated explicitly that he chose not to obtain a warrant because the computer, and therefore its data, were the property of the School Board:

> [Crown Counsel Mr. Roy]. And did you consider obtaining a search warrant?
>
> A. Yes, I did, sir.
>
> Q. And whose decision was it to make with respect to whether or not you would be obtaining a search warrant? Did you consult with anyone else?
>
> A. No, that was my decision, sir.
>
> Q. And why did you decide not to obtain a search warrant?
>
> A. It was my belief that the laptop in question was the property of the Rainbow District School Board, that Mr. Slywchuk had said that it was a teacher or a staff computer, that the sticker on the bottom of the laptop indicated it was property of Rainbow District School Board, and at that point I was advised that it was their property. . . .
>
> . . .
>
> Q. Now would your approach have been different if you were seizing a computer from a residence?
>
> A. In a residence there are several users on computers. This is a personal computer as opposed to a business computer with a property. Most of us don't put a "Property of Tim Burtt" on the back of my computer as opposed to a property of an employer. So I would look in my household and there are three, four people who could use my computer and I believe that each one of them would have a privacy interest because my son may be chatting with someone or somebody in a household may be chatting and they may claim that they have some kind of privacy. I would get a search warrant even if, use an example, a wife catches her husband doing

something and says I don't want this computer, I want you to do this because I caught him doing something illegal, and it's in my possession already at headquarters, I would get a warrant for it in that time because I would be respecting the privacy of all those people on that personal computer.

Q. Did you consider whether or not Richard Cole had any expectation of privacy in that computer?

A. I did consider that. The information that I was receiving was that it was the School Board's computer and that was their property. I had never received any information in regards to Mr. Cole owning that computer or that he had any privileged material. And I've dealt with cases where there have been privileged material on a laptop or on a computer. And the only information I had received about any private material that was on that computer came from Mr. Bourget [the school principal] and that was in regards to some images of Mr. Cole's — personal images of his wife and that was the only information I had in regards to any private information there.

. . .

[Defence Counsel Mr. Keaney]. Okay. And you decided not to get a search warrant before looking at that CD called the temporary Internet folder. Why?

A. Because of the same reasons as I explained with the laptop, that I believe that the data and the images were all part of that laptop and that that laptop belonged to the Rainbow District School Board.

. . .

A. . . . if I believe that there's a privacy interest I would get a warrant . . . for it, but based on the information I collected up until the examination of the computer, including the procedures, the data contained within and that would be, I guess, a subject to review, the data contained and created within being the Board's property, what they call their property, I didn't believe that that data belonged to Mr. Cole. [Emphasis added.]

[117] Apart from vague references to "privileged material", the distinction that D.C. Burtt drew between the search of a shared home computer and that of a work computer was the fact that the laptop belonged to the School Board. He

acknowledged that if he were searching a home computer used by several people, he would obtain a warrant "because [he] would be respecting the privacy of all those people on that personal computer". The distinction for him appears to have been that "[m]ost of us don't put a 'Property of Tim Burtt' on the back of [a] computer as opposed to a property of an employer." Indeed, immediately after this statement, D.C. Burtt reaffirmed that he did not get a warrant in Mr. Cole's case *because of the School Board's ownership of the laptop*. This echoes the repeated statements he made throughout his testimony to justify his failure to get a warrant or to conduct a further inquiry into the privacy interests at play.

[118] Despite acknowledging that there could be personal information on Mr. Cole's computer, and despite being told by the principal of the school that Mr. Cole kept personal photographs on it, there is no evidence that D.C. Burtt took any steps to discover the extent of the private information on Mr. Cole's computer before effecting a warrantless search.

[119] D.C. Burtt acknowledged that he knew about the private use that Mr. Cole made of the laptop before he looked at the content of the CDs. He knew that Mr. Cole had a password to his computer. He had also received statements confirming that the photos were in a hidden folder, that teachers regularly kept personal information on their laptops and that Mr. Cole specifically had "personal private information on his computer", namely the photos of his wife. In fact, D.C. Burtt even acknowledged that, in conducting a warrantless search of Mr. Cole's

workplace computer, he knew there could be "personal stuff on there", and would make efforts to avoid it:

> Business computer or any computers may have some personal stuff on there. I can even use an example from our own computers that I know that officers may check a website and may send an e-mail. So some people will have a personal folder or a personal picture or something like that. I'll respect that because it's not what I'm looking for. Essentially I've been given information in regards to possible child pornography. Mr. Cole's wife is not part of the investigation and it's — when the forensic images obtain . . . It's hard to explain but the whole computer, when the . . . The forensic program takes all of the images, not just from one area. It takes it so that it can recreate a proper image. So when all those images come in I'm not particularly — 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. [Emphasis added.]

[120] D.C. Burtt would not have been able to rely on the School Board's ownership of an office desk for a warrantless search of Mr. Cole's personal files in the desk's drawer, in complete disregard for Mr. Cole's privacy interests (see *Buhay*). The same should be true of Mr. Cole's school-owned laptop.

[121] There were also no exigent circumstances or other legitimate reasons that forced the police to proceed without a warrant. As the trial judge noted, "[h]ad the legal route to accessing the data in that computer been followed, it is likely that it could have been obtained without alerting Richard Cole about what was transpiring." There was therefore no urgent need on the part of the police to preserve the evidence.

[122] In his testimony, D.C. Burtt accepted that once he received the CDs and the laptop, he was confident that they would remain uncompromised, that their integrity would not be at issue, and that there was ample time to get a warrant. In fact, though he looked at the CDs immediately after seizing the materials on June 28, the laptop was not sent for forensic analysis until August 18, nearly two months later. This too weighs in favour of exclusion.

[123] It is also uncontested that D.C. Burtt not only had ample time to obtain a warrant, he had reasonable and probable grounds to do so. The relevance of this factor was recently discussed in *R. v. Côté*, [2011] 3 S.C.R. 215, where the Court said that the failure to obtain a warrant can either be a mitigating or an aggravating factor under the first branch of the *Grant* test, depending on whether the police had a "legitimate" reason for it (*R. v. Grant*, [2009] 2 S.C.R. 353). In this case, it seems to me that the "legitimacy" of the warrantless search hinges on the finding that D.C. Burtt's good faith was compromised by his disregard for the established law. Since I see no reason justifying his decision not to get a warrant, this factor too mandates in favour of exclusion.

[124] The second aspect of the *Grant* test considers the impact on the *Charter*-protected interests of the accused. This factor "calls for an evaluation of the extent to which the breach actually undermined the interests protected by the right infringed" (*Grant*, at para. 76). The interest in this case is privacy. *Grant*, *R. v. Harrison*, [2009] 2 S.C.R. 494, and *Côté* address the key relevant concerns at play in

determining the impact of a breach of a privacy interest in this case: the reasonable expectation of privacy and the extent of the intrusion.

[125] The reasonable expectation of privacy is central to assessing the impact of the breach on the accused's *Charter*-protected interests. Even if it can be said that there is a diminished expectation of privacy in a workplace computer, this is not the end of the inquiry. The record shows that teachers at the school kept a great deal of personal information on their computers, a fact that was known both to the school and to D.C. Burtt prior to the police search. Mr. Cole himself kept personal photos, financial records, tax records, and information about a property he owned on his computer. The search also included Mr. Cole's Internet browsing history, which would provide an extensive, unfiltered view of many aspects of his life. As Justice Fish recognized, the information that was available on the search of Mr. Cole's computer was "meaningful, intimate, and organically connected to his biographical core".

[126] The substantial amount of private information which was seized by the police from Mr. Cole's computer meant that it was a highly intrusive search. In other words, regardless of whether there is a diminished expectation of privacy in a workplace computer, the *extent* of the seizure in a given case should be relevant under s. 24(2). In *Harrison*, the Court asked whether "the breach [was] merely transient or trivial in its impact" and considered it a mitigating fact that, "[h]ad it not turned up incriminating evidence, the detention would have been brief" (paras. 28 and 30). In

Côté, the Court noted that the police had conducted a two-hour warrantless search of the accused's home (para. 85). And in *Morelli*, the breadth of the search of the accused's computer was significant to the analysis (paras. 104-5).

[127] The warrantless search and seizure in this case included not only the impugned photos, but also the computer and a copy of the data on the hard drive. In other words, it had no restrictions as to scope. As a result, regardless of any diminished reasonable expectation of privacy in a workplace computer, the *extent* of the search of Mr. Cole's hard drive and browsing history was significant, which weighs in favour of exclusion.

[128] The fact that the police had reasonable and probable grounds to obtain a search warrant and discover the evidence does little to attenuate the intrusiveness of the search that actually occurred. As this Court explained in *Côté*,

> the absence of prior judicial authorization still constitutes a significant infringement of privacy. Indeed, it must not be forgotten that the purpose of the *Charter*'s protection against unreasonable searches is to prevent them before they occur, not to sort them out from reasonable intrusions on an *ex post facto* analysis: *R. v. Feeney*, [1997] 2 S.C.R. 13, at para. 45. Thus, prior authorization is directly related to, and forms part of, an individual's reasonable expectation of privacy. [para. 84]

[129] The third and final factor in *Grant* is society's interest in an adjudication on the merits, which "asks whether the truth-seeking function of the criminal trial process would be better served by admission of the evidence, or by its exclusion" (para. 79). Three considerations have been emphasized by the Court in weighing this

factor: the reliability of the evidence, its importance to the prosecution's case, and the seriousness of the offence.

[130] First, "[i]f a breach . . . undermines the reliability of the evidence, this points in the direction of exclusion of the evidence" (*Grant*, at para. 81). While I agree with Justice Fish that the evidence in this case is reliable, a factor arguing in favour of admission, its importance to the prosecution's case is, it seems to me, minimal, and it can hardly be said to reach the level described in *Grant* of "effectively gut[ting] the prosecution" (para. 83).

[131] There is little evidence in this case about the particular relevance of the laptop and Internet browsing history, especially given that the pornographic photographs themselves, as well as the screenshot showing their location on Mr. Cole's computer, were both admitted. The Crown suggests that the information in the laptop, including the metadata accompanying the photos (data stored on each file that records when it was created and altered) and the Internet browsing history, help establish the context in which the files were downloaded and whether the files were viewed, copied or transmitted.

[132] At best, the Crown's need for Mr. Cole's *entire* hard drive and his browsing history in order to establish possession of child pornography, is highly speculative. In *Morelli*, the Court held that in order to be guilty of possession of child pornography, "one must knowingly acquire the underlying data files and store them in a place under one's control", such as by storing it on the hard drive (para. 66).

That knowledge and control can be inferred if the pornography is found in a folder where users typically keep their personal files.

[133] In Mr. Cole's case, the pornographic photos were stored in a folder under "My Documents" and the screenshot records their location. This location supports an inference that they were deliberately placed there by Mr. Cole. As a result, the Crown may well be able to establish possession without the metadata and browsing history.

[134] Finally, while the seriousness of the offence is a relevant factor to consider, *Grant* observed that it "has the potential to cut both ways". Section 24(2) is focussed on the longer-term reputation of the administration of justice. As a result, "while the public has a heightened interest in seeing a determination on the merits where the offence charged is serious, it also has a vital interest in having a justice system that is above reproach, particularly where the penal stakes for the accused are high" (para. 84). This statement was reaffirmed in *Harrison* and *Côté*, cases where the Court excluded evidence that was central to the prosecution of a serious offence. It seems to me that the result of these decisions is to seriously attenuate the impact of the seriousness of the offence in the s. 24(2) analysis.

[135] This brings us to balancing these factors. The *Charter*-infringing conduct in this case was serious in its disregard for central and well-established *Charter* standards. Nor were there any exigent circumstances or other legitimate reasons preventing the police from getting a warrant. The impact of the breach on Mr. Cole's *Charter*-protected interests, even assuming that his reasonable expectation of privacy

was reduced because it was a workplace computer, was significant given the extent of the intrusion into his privacy. And while the evidence in this case is reliable, its importance to the prosecution's case is at best speculative. Balancing these factors, and in light of the deference owed to trial judges in applying s. 24(2), it seems to me that the trial judge was reasonable in excluding the evidence.

[136] I would dismiss the appeal.

Appeal allowed, ABELLA J. *dissenting.*

Solicitor for the appellant: Attorney General of Ontario, Toronto.

Solicitors for the respondent: Addario Law Group, Toronto; Ruby Shiller Chan, Toronto.

Solicitor for the intervener the Director of Public Prosecutions: Public Prosecution Service of Canada, Edmonton.

Solicitor for the intervener the Attorney General of Quebec: Attorney General of Quebec, Québec.

Solicitors for the intervener the Criminal Lawyers' Association (Ontario): Dawe & Dineen, Toronto.

Solicitors for the intervener the Canadian Civil Liberties Association: Lax O'Sullivan Scott Lisus, Toronto.

Solicitors for the intervener the Canadian Association of Counsel to Employers: Hicks Morley Hamilton Stewart Storie, Toronto.