File No. 34268

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

B E T W E E N

HER MAJESTY THE QUEEN

Appellant (Respondent)

– and –

RICHARD COLE

Respondent (Appellant)

– and –

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

Interveners

FACTUM OF THE INTERVENER CRIMINAL LAWYERS' ASSOCIATION (ONTARIO)

[*Rules of the Supreme Court of Canada,* Rule 37]

TABLE OF CONTENTS

PART I: STATEMENT OF FACTS

1. The Crown is appealing to this Court from the decision of the Ontario Court of Appeal allowing the Respondent's appeal and making an order pursuant to s. 24(2) of the *Charter* excluding certain evidence at his new trial. On April 11, 2012 Mr. Justice Moldaver granted Intervener status to the Criminal Lawyers' Association (Ontario) ["the CLA"], along with permission to file a 10-page factum.

Order of Moldaver J., dated April 11, 2012

2. The CLA accepts the facts as set out in the Appellant and Respondents' facta.

PART II: THE CLA'S POSITION ON THE QUESTIONS IN ISSUE

3. The Appellant identifies three "points in issue":

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

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

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

On the first issue, the CLA agrees with and adopts the Respondent's submissions concerning the applicable legal principles, and makes further submissions as set out below. On the second issue, the CLA agrees with and adopts the Respondent's submissions concerning the applicable law but takes no position with respect to the application of the law to the particular facts of this case. On the third issue, the CLA takes no position with respect to the exclusion of the particular evidence in this case but makes submissions concerning the governing principles under s. 24(2) of the *Charter*. Finally, the CLA makes submissions in response to the intervener Canadian Association of Counsel to Employers's suggestion that this Court should "articulate a broad and clear corresponding right of employer access" to employees' private information stored on employer-owned computers.

Appellant's Factum, pp. 10-11
Factum of the Canadian Association of Counsel to Employers (Intervener), ¶4

PART III: STATEMENT OF ARGUMENT

A. Private Contracts and *Charter* Protection Against Unreasonable State Intrusions on Privacy

4. The Appellant argues that employers' formal policies concerning the use of employer-owned computers and similar devices should be treated as the "key contextual factor" in the s. 8 reasonable expectation of privacy analysis. The CLA acknowledges that when such policies exist they will be relevant, but submits that they should not be treated as decisive. There are two main reasons for this, both of which can be linked to this Court's recognition that "[e]xpectation of privacy is a normative rather than a descriptive standard".[1]

10 *R. v. Tessling,* [2004] 3 S.C.R. 432 at ¶42 [*Appellant's Book of Authorities*, Vol. II, Tab 63]
R. v. M.(A.) 2008 SCC 19, [2008] 1 S.C.R. 569 at ¶65 *per* Binnie J. [*Appellant's Book of Authorities*, Vol. I, Tab 19]
R. v. Patrick, 2009 SCC 17, [2009] 1 S.C.R. 579 at ¶12 [*Appellant's Book of Authorities*, Vol. II, Tab 51]
R. v. Gomboc, 2010 SCC 55, [2010] 3 S.C.R. 211at ¶34, *per* Deschamps J., at ¶115, *per* McLachlin C.J.C. and Fish J., (dissenting in the result) [*Appellant's Book of Authorities*, Vol. I, Tab 38]

5. First, employees' reasonable expectations of privacy over personal data stored on employer-owned electronic devices should be seen as shaped primarily by the actual practices in their workplace, particularly when their employer's formal written policies are ambiguous or have never been strictly applied. In the case at bar, the Summary Conviction Appeal Court
20 reasoned that an employee "who does not object and continues his or her employment" in the face of an asserted right by his employer to "monitor his work, email and data stored on his computer drives" should be deemed to have "waived his right of privacy to this data".[2] From a normative perspective, it is not realistic to expect employees to quit their jobs whenever their employer introduces an objectionable written policy, particularly if this new policy is never actually implemented in practice. In this regard, it is submitted that the Ontario Court of Appeal was correct in the case at bar to give the "conventions and customary use [of board-owned computers] by teachers"[3] primacy over the board's formal written policy, in light of the ambiguity of the board's privacy policy[4] and the factual finding at trial that the board's actual practice was to give teachers exclusive use of board-owned computers and expressly permit them

---

[1] *R. v. Tessling, infra* at ¶42; *R. v. M.(A.), infra* at ¶65 *per* Binnie J.; *R. v. Patrick, infra* at ¶12; *R. v. Gomboc, infra* at ¶34, *per* Deschamps J., at ¶115, *per* McLachlin C.J.C. and Fish J., (dissenting in the result).
[2] Decision of Kane J., Superior Court of Justice, ¶33 [*Appellant's Record,* Vol. I, p. 43]
[3] Reasons for Judgment, Court of Appeal for Ontario, at ¶38 [*Appellant's Record,* Vol. I, p. 61]
[4] The school board's policy declared that all data on board-owned computers (including e-mails) belonged exclusively to the board, but simultaneously stated that e-mails were "considered private". See *Appellant's Record,* Vol. II, pp. 174-76.

to use these machines for personal purposes.[5] Where evidence establishes that employees have well-founded expectations of privacy based on their employer's actual past practices, these expectations should be seen as "reasonable" for s. 8 *Charter* purposes.

> Decision of Kane J., *Appellant's Record*, Vol. I, p. 43
> Reasons for Judgment, Court of Appeal for Ontario, *Appellant's Record*, Vol. 1, pp. 61-62

6. Second, and more generally, this Court should continue to exercise caution when considering contractual terms as a factor in s. 8 *Charter* privacy analysis. The amount of privacy Canadians should be entitled to expect *vis-à-vis* the state is a normative question, and one that is far too important to be left solely to employers or other commercial businesses to decide. As Deschamps J. observed in her plurality reasons in *R. v. Gomboc, supra* (at para. 33):

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

Modern consumers are inundated with "terms of agreement" and "privacy policies" that they must sign or "click to accept" in order to go about their day-to-day lives. The reality is that most people never read these documents, let alone parse them minutely and appreciate their every potential nuance. Whatever effect these documents might have when it comes to determining private rights between the parties, there is no good policy reason to treat them as determinative of individual privacy rights *vis-à-vis* the state. Were it otherwise, it would be all to easy for the police to circumvent s. 8 of the *Charter* by persuading private companies to insert terms into contracts of adhesion that are specifically designed to allow the police warrantless access to information that would otherwise be considered private and constitutionally protected. This is not a purely hypothetical concern, but is something that has actually happened in recent years in the context of private customer information in the hands of internet service providers.[6]

> *R. v. Gomboc, supra* at ¶33
> A. Slane & L. Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" 57 C.L.Q. 486 (2011) [*CLA's Book of Authorities*, Tab 1]

---

[5] See Ruling on *Voir Dire* of Guay J., Ontario Court of Justice, *Appellant's Record,* Vol. I, pp. 21-22.

[6] See Slane and Austin, *infra*, discussing a recent agreement between a consortium of internet service providers (ISPs) and law enforcement agencies pursuant to which the ISPs agreed to insert into their consumer internet service contracts terms that are specifically intended to allow the ISPs to grant the police warrantless access to certain information (internet protocol address histories) when they are investigating child pornography offences. In all other contexts, including police investigations of other offences and requests by private parties, the ISPs this same information as private and will produce it only when compelled by a warrant or court order.

7. In this regard, while the CLA agrees with the Respondent that many of the US cases relied on by the Appellant are distinguishable on the grounds that they involved much clearer employer denials of the existence of employee privacy rights than are found in the case at bar,[7] the CLA goes further and urges caution when it comes to adopting American precedents in this area. From a normative perspective, it is far from clear that employers *should* be able to deny privacy to their employees merely by giving them advance notice that their private conversations and communications using company-owned electronic devices will be monitored. Canadian labour relations traditions are very different from those in the United States, and Canadian courts should be cautious before adopting US precedents that reflect a very different view of the respective powers and rights of employers and employees. Caution is particularly warranted here in view of the reluctance of the US Supreme Court to endorse the lower court precedents relied on by the Appellant. In his plurality opinion in *Ontario v. Quon*, *infra* Kennedy J. stated:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. …. In *Katz* , the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. … It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices. [Citations omitted]

Justice Kennedy noted further that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior", and observed that it is "[a]t present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."

Ontario v. Quon, 130 S.Ct. 2619 at pp. 2629-30 (2010) [*Appellant's Book of Authorities*, Vol. I, Tab 16]

8. Finally, it is important to emphasize that the issue here is whether employees should have an expectation of privacy *vis-à-vis* the state, not with respect to their own employer. In other contexts this Court has recognized that privacy is relational, and that people who cede their privacy to a limited class of people for a limited purpose do not necessarily relinquish their s. 8 *Charter* rights to be secure against unreasonable intrusions on their privacy by state agents.[8] It is also important to recognize the full implications of the Appellant's argument that the Respondent

[7] Appellant's Factum, ¶43-45; Respondent's Factum, ¶43
[8] See, *e.g., R. v. Colarusso, infra*; *R. v. Buhay, infra*; *R. v. Wong, infra*.

should be seen as having no reasonable expectation of privacy over personal data stored on the school board-owned computer. While in the case at bar the police became interested in the computer only because a board employee had already accessed the data (lawfully, according to the Ontario Court of Appeal) and found suspicious images, if the Appellant's main position is correct this circumstance would be rendered irrelevant: the police would be able to seize and search the computer from the school without any basis for suspicion or anyone's consent, and in the Respondent's ensuing criminal trial neither he nor the Board would have had standing to object to the blatantly illegal police conduct.[9] Such a result would surely bring the administration of justice into disrepute.

10 *R. v. Colarusso,* [1994] 1 S.C.R. 51 [*Appellant's Book of Authorities*, Vol. I, Tab 26]
R. v. Buhay, [2003] 1 S.C.R. 631 [*Appellant's Book of Authorities*, Vol. I, Tab 26]
R. v. Wong, [1990] 3 S.C.R. 36 [*Appellant's Book of Authorities*, Vol. II, Tab 68]

B. Section 24(2)

1) The failure to seek a warrant in circumstances of legal uncertainty increases the seriousness of the breach

9. In its submissions on the *Grant* exclusionary analysis, the Appellant relies heavily on the assertion that privacy over workplace computers was an "undeveloped area of the law", and that even if the police actually needed a warrant their failure to seek one here was an "understandable" mistake that lessens the gravity of the *Charter* breach.[10] The CLA submits that
20 this Court should take the opposite approach. When the law is unclear and the circumstances are not exigent, the police should be expected to err on the side of caution and seek prior judicial authorization. If they get a warrant in circumstances where it is later established by the courts that they did not really need one, they will have suffered some minor inconvenience. On the other hand, if they routinely decline to seek warrants until they are specifically told by the courts that a warrant is required, the privacy and *Charter* rights of an unknown number of people will have been infringed for no good reason. As this Court recently explained in *R. v. Cote, infra*, even when the police manifestly have sufficient grounds for a warrant, their failure to obtain prior judicial authorization is *in itself* a breach of privacy:

---

[9] If the Respondent has no expectation of privacy over either the contents of the computer hard drive or the place from which the computer was seized, he would have no standing to challenge the lawfulness of the seizure and ensuing search. Conversely, the board would have no standing at the Respondent's trial, although it could conceivably seek some remedy in separate proceedings.
[10] Appellant's Factum, ¶98(a)-(d).

> 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. [Emphasis added.]
>
> *R. v. Cote* [2011] 3 S.C.R. 215 at ¶84 [*Appellant's Book of Authorities,* Vol. I, Tab 28]

10. The CLA submits that when police officers have chosen not to seek a warrant in circumstances where it is later held that the law required one, this should generally be seen as aggravating the seriousness of the resulting *Charter*-infringing state conduct, absent specific indicia of good faith (such as exigent circumstances or reasonable reliance on subsequently overturned judicial authority). If the police do not bother to get a warrant because they mistakenly hope or assume that the law will evolve in their favour, this suggests a lack of respect for the prior judicial authorization regime mandated by s. 8 of the *Charter*. As Lamer J. stated in *R. v. Collins*, *infra* a "failure to proceed properly when that option was open to them tends to indicate a blatant disregard for the *Charter*, which is a factor supporting the exclusion of the evidence."

> *R. v. Collins* [1987] 1 S.C.R. 265 at ¶38 [*Appellant's Book of Authorities,* Vol. I, Tab 27]

2) Provisional s. 24(2) rulings

11. In the judgement on appeal, the Ontario Court of Appeal stated that although it was ordering that certain evidence be excluded under s. 24(2) at the Respondent's new trial:

> … 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.[11]

The Appellant embraces this suggestion as a "welcome development" in the s. 24(2) jurisprudence.[12] The CLA takes a contrary view, submitting that the Court of Appeal's suggestion that pre-trial exclusionary should be subject to revision if the importance of the evidence to the Crown's case unexpectedly increases is both contrary to principle and unworkable in practice.

12. As a matter of principle, the defence is entitled to know by the close of the Crown's case what the evidence against him or her consists of. As Lamer C.J.C. said for the Court in *R. v. Underwood*, *infra* at ¶6:

---

[11] Reasons for Judgment, Ontario Court of Appeal, ¶92, *Appellant's Record,* Vol. I, p. 86
[12] Appellant's Factum, ¶98(j).

> Our criminal process is based upon the principle that before the accused calls evidence in his own defence, he must have knowledge of the case to be met. … The "case-to-meet" principle is a fundamental tenet of the criminal justice system, firmly rooted in the common law and an integral part of the principles of fundamental justice … which are protected by s. 7 of the *Canadian Charter of Rights and Freedoms*. It is part of the broader principle against self-incrimination, which has its roots in the presumption of innocence and the power imbalance between the state and the individual. [Citations omitted.]

Critical tactical decisions such as whether or not to call the defendant or other defence witnesses, or call a defence at all, will frequently depend on whether or not unconstitutionally obtained evidence has been excluded. For instance, absent "very limited circumstances" it would be "grossly unfair" to revisit a s. 24(2) ruling excluding the accused's statement on the grounds that the accused has taken the witness stand, thereby making the excluded statement more "important to the truth-seeking function" (see, *e.g., R. v. Calder, infra*). Such an approach would turn pre-trial s. 24(2) rulings into a potential trap for the accused.

R. v. Underwood, [1998] 1 S.C.R. 7 at ¶6 [*CLA's Book of Authorities*, Tab 3]
R. v. Calder [1996] 1 S.C.R. 660 at ¶35 [*CLA's Book of Authorities*, Tab 2]

13. While revisiting s. 24(2) exclusionary rulings before the Crown has closed its case will not offend the case to meet principle, it in many cases it will still cause real unfairness to the defence. Tactical defence decisions made while the Crown's case is unfolding – such as whether and in what manner to cross-examine particular Crown witnesses – are often strongly influenced by pre-trial evidentiary rulings. If a pre-trial exclusionary ruling is reversed midway through a trial, the defendant will often be severely prejudiced unless the trial court takes extensive remedial steps (*e.g.*, recalling certain witnesses and permitting further cross-examination of them). These remedial steps will inevitably disrupt and lengthen trials. The CLA submits that there is no reason to depart from this Court's majority holding in *Calder* that pre-trial decisions excluding evidence under s. 24(2) should generally be considered final, absent "very special circumstances".

R. v. Calder, supra

14. The Ontario Court of Appeal's suggestion that s. 24(2) exclusionary rulings should be reviewable mid-trial is particularly troubling insofar as the Court's decision can be read as suggesting that excluded evidence might sometimes become admissible if the rest of the Crown's case proves to be insufficient to support a conviction. The third prong of the *Grant* analysis must not be understood as permitting exclusion only where the Crown can still secure a conviction by

other means. Such an approach would suggest to the public that *Charter* rights will be enforced only when this can be done at no cost. This would "send the message that individual rights count for little", contrary to this Court's holding in *Grant*.

R. v. Grant [2009] 2 S.C.R. 353 at ¶71 [Appellant's Book of Authorities, Vol. I, Tab 39]

C. Response to the Position of the Canadian Association of Counsel to Employers ("CACE")

15. The intervener Canadian Association of Counsel to Employers ("CACE") argues that if this Court recognizes a reasonable expectation of privacy in the case at bar, it should also "articulate a broad and clear corresponding right of employer access" to private information stored on employer-owned computers.[13] It is submitted that this suggestion is ill-considered in several respects.

16. First, the "reasonable expectation of privacy" analysis in s. 8 *Charter* cases has a narrow and specific purpose: it determines whether or not a *Charter* claimant's s. 8 rights were engaged by the particular state intrusions at issue. Most employers are not state actors, and are thus not bound by the *Charter*. Recognizing that employees can have a protected s. 8 *Charter* interest in personal data stored on an employer-owned computer has no direct bearing one way or the other on the separate question of whether and in what circumstances a non-state employer can access this data. Rather, the answer to this latter question will turn on the case-specific interplay of legislation, contractual terms and collective agreements, and labour law jurisprudence. It is neither necessary or advisable for this Court to address these entirely unrelated issues in this case, let alone to create a sweeping "right of employer access" as the CACE urges.

17. Second, while state employers such as the school board in the case at bar are presumptively bound by the *Charter*, the Ontario Court of Appeal concluded that the school board technician's actions *in this case* did not violate the Respondent's s. 8 *Charter* rights. The Court did not purport to decide whether or not the Respondent's rights would have been infringed if the technician had accessed his private files for a different reason or in a different manner, since that question did not arise in the case. The Respondent has not cross-appealed, and the correctness of this aspect of the Ontario Court of Appeal's judgment and its underlying reasoning are thus not in issue before this Court. For both reasons, it would be inadvisable for

[13] Factum of the Canadian Association of Counsel to Employers, ¶4.

this Court to make any sweeping statements about the "right" of state employers to access private employee information in other contexts, such as the hypothetical situations set out by the intervener CACE at para. 25 of its factum, which do not arise on the facts here and were not argued or considered in the courts below. The intervener's proposed employer "right" raises a number of significant legal and policy issues that should be fully argued in a case where they actually arise, and where this Court has the benefit of judgments from lower courts and specialized labour law tribunals.[14]

> Factum of the Canadian Association of Counsel to Employers, ¶25

PART IV: SUBMISSIONS ON COSTS

10 18. The CLA does not seek costs and asks that none be awarded against it.

PART V: NATURE OF THE ORDER REQUESTED

19. The CLA seeks leave to make oral submissions of not longer than 10 minutes. The CLA takes no position on the disposition of this appeal, which turns on an assessment of the particular facts of this case.

---

[14] For instance, in the Intervener's first three hypotheticals it is not apparent that the employer would have any legitimate justification for accessing or reading sent or received emails in the employee's account that were of an obviously personal nature. Moreover, even if it is assumed that s. 8 the *Charter* should not prevent state employers from accessing employees' personal email and files in some or all of these hypothetical situations, there are several alternative jurisprudential routes by which this conclusion could be reached (*i.e.,* it may be because employees have no reasonable expectation of privacy *vis-à-vis* their employers in this context, it may be because they are deemed to have waived their s. 8 *Charter* rights, or it may be because the employer's interference with employee privacy interests is found to be "reasonable" and thus compliant with s. 8). The CLA submits that this Court should not attempt to resolve these issues in a case where the issue does not arise and has not been fully argued.

ALL OF WHICH IS RESPECTFULLY SUBMITTED THIS 30th DAY OF APRIL, 2012.

_____
JONATHAN DAWE

_____
MICHAEL DINEEN
10 DAWE & DINEEN
171 John Street, Suite 101
Toronto, Ontario
M5T 1X3

OF COUNSEL FOR THE INTERVENER
CRIMINAL LAWYERS' ASSOCIATION
(ONTARIO)

PART VI: AUTHORITIES TO BE CITED

PARAGRAPHS