CACE News Release
v.4

CAN EMPLOYEES EXPECT PORNOGRAPHY ON A WORK COMPUTER TO BE PRIVATE?

Canadian Association of Counsel to Employers intervenes in Supreme Court of Canada Case

Toronto – In a case involving a teacher and nude sexually explicitly images of a grade 10 student, the Canadian Association of Counsel to Employers (CACE) has intervened before the Supreme Court on the case, *R. v. Cole*, on the issue of privacy and work computers.

"This is more than a criminal case because the Court will be asked to weigh competing employer and employee interests. It has the potential to answer some very important questions for employers who are not already regulated by privacy legislation," said Daniel J. Michaluk, a Partner at Hicks Morley who has been retained by CACE to represent it on this matter. "Among the questions needed to be answered are; when does personal use invite a reasonable expectation of privacy? Can employer policy reduce or eliminate that expectation? And if an employee does have a reasonable expectation of privacy what rights do employers retain?"

CACE will make representations to help the Court make a sound decision for employers that rests on a full understanding of the function and significance of a work information system. It will argue:

- A work computer is part of a system and not a personal storage device,
- A work information system serves a critical business function,
- A work information system is a repository of information that must be secured, and
- Employers need a broad and clear right of access to information on their system.

"Canadian employers, large and small, are routinely faced with the question of privacy as it relates to computers that are part of the employer's networks but are used by employees," said Andrew Finlay, Chair of CACE's Advocacy Committee. "We are hopeful that this case will ensure employers have continued access to the information they need and clarify expectations for the many employees who use work computers and electronic devices for personal purposes."

File Number: 34268

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

BETWEEN:

HER MAJESTY THE QUEEN

Appellant

- and -

RICHARD COLE

Respondent

- and -

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

Interveners

FACTUM OF THE CANADIAN ASSOCIATION OF COUNSEL TO EMPLOYERS

DANIEL MICHALUK and
JOSEPH COHEN LYONS
Hicks Morley Hamilton Stewart Storie LLP
77 King Street West, 39th Floor
Box 371, TD Centre
Toronto, ON M5K 1K8
Tel: 416-864-7253
Fax: 416-362-9680
E-mail: daniel-michaluk@hicksmorley.com
E-mail: joseph-cohen-lyons@hicksmorley.com

Counsel for the Intervener Canadian Association of Counsel to Employers

SIOBHAN O'BRIEN
Hicks Morley Hamilton Stewart Storie LLP
150 rue Metcalfe St.
Suite 2000
Ottawa, ON K2P 1P1
Tel: 613-369-8411
Fax: 613-234-0418
E-mail: siobhan-obrien@hicksmorley.com

Ottawa Agents for the Intervener Canadian Association of Counsel to Employers

ORIGINAL TO:

THE REGISTRAR
Supreme Court of Canada
301 Wellington ST.
Ottawa, ON K1A OJ1

COPIES TO:

AMY ALEA and FRANK AU
Attorney General of Ontario
10th Floor, Crown Law Office Criminal
720 Bay Street
Toronto, ON M5G 2K1
Tel: (416) 362-4187
Fax: (416) 326-4656
Email: amy.alyea@ontario.ca

Agent for the Appellant

ROBERT E. HOUSTON, Q.C.
Burke Robertson
70 Gloucester Street
Ottawa, ON K2P 0A2
Tel: (613) 566-2058
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Agent for the Appellant

FRANK ADDARIO
Addario Law Group
Barristers and Solicitors
Suite 101 – 171 John Street
Toronto, ON M5T 1X3
Tel: (416) 979-6446
Fax: (866) 714-1196
Email: faddario@addario.ca

Co-Counsel for the Respondent

COLLEEN BAUMAN
Sack Goldblatt Mitchell LLP
Barristers and Solicitors
Suite 500 – 30 Metcalfe Street
Ottawa, ON K1P 5L4
Tel: (613) 235-5327
Fax: (613) 235-3041
Email: cbauman@sgmlaw.com

Agent for the Respondent

GERALD CHAN and NADER R. HASAN
Ruby Shiller Chan
11 Prince Arthur Avenue
Toronto, ON M5R 1B2
Tel: (416) 964-9664
Fax: (416) 964-8305
Email: nhasan@rubyshiller.com

Co-Counsel for the Respondent

RON REIMER and MONIQUE DION
Director of Public Prosecutions
700, 10423 – 101 Street
Edmonton, AB T5H 0E7
Tel: (780) 495-4079
Fax: (780) 495-6940

Counsel for the Intervener, Director of Public Prosecutions

FRANCOISE LACASSE
Director of Public Prosecutions
284, rue Wellington
2ième étage
Ottawa, ON K1A 0H8
Tel: (613) 957-4770
Fax: (613) 941-7865
Email: flacasse@ppsc-sppc.gc.ca

Agent for the Intervener, Director of Public Prosecutions

DOMINIQUE A. JOBIN
Attorney General of Quebec
1200, route de l'Église, 2e étage
Sainte-Foy, Quebec G1V 4M1
Tel: (418) 643-1477 x 20788
Fax: (418) 644-7030
Email: dominique-a.jobin@justice.gouv.gov.gc.ca

Counsel for the Intervener, Attorney-General of Quebec

PIERRE LANDRY
Noel & Associates, s.e.n.c.r.l.
111, rue Champlain
Gatineau, Quebec J8X 3R1
Tel: (819) 771-7393
Fax: (819) 771-5397
Email: p.landry@noelacssocies.com

Agent for the Intervener, Attorney-General of Quebec

JONATHAN DAWE and MICHAEL DINEEN
Dawe & Dineen
171 John Street, Suite 101
Toronto, ON M5T 1X3
Tel: (416) 649-5058
Fax: (416) 352-7733
Email: jdawe@dawedineen.com

Counsel for the Intervener, Criminal Lawyers' Association (Ontario)

ED VAN BEMMELL
Gowling Lafleur Henderson LLP
160 Elgin Street
Suite 2600
Ottawa, ON K1P 1C3
Tel: (613) 223 1781
Fax: (613) 563-9869
Email: ed.vanbemmell@gowlings.com

Agent for the Intervener, Criminal Lawyers'' Association (Ontario)

JONATHAN C. LISIUS and MICHAEL PERLIN
Lax O'Sullivan Scott Lisius LLP
145 King Street West
Suite 1920
Toronto, ON M5H 1J8
Tel: (416) 598-1744
Fax: (416) 598-3730
Email: jlisus@counsel-toronto.com

Counsel for the Intervener,
Canadian Civil Liberties Association

HENRY S. BROWN, Q.C.
Gowling Lafleur Henderson LLP
2600 – 160 Elgin St.
Ottawa, ON K1P 1C3
Tel: (613) 233-1781
Fax: (613) 788-3433
Email: henry.brown@gowlings.com

Agent for the Intervener,
Canadian Civil Liberties Association

File Number: 34268

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

BETWEEN:

HER MAJESTY THE QUEEN

Appellant

- and -

RICHARD COLE

Respondent

- and -

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

Interveners

FACTUM OF THE CANADIAN ASSOCIATION OF COUNSEL TO EMPLOYERS

Table of Contents

PART I – OVERVIEW

1. The reasonableness of an expectation of privacy in the content of a work-issued computer should be judged in light of the function of the information system of which the computer is a part.

2. The Court of Appeal for Ontario failed to undertake such an assessment in finding that the Respondent had a reasonable expectation of privacy in the contents of his work-issued laptop. The Court focussed heavily on facts related to the Respondent's personal use - his possession of the laptop on weekends and the kind of sensitive personal information he might have stored on the laptop. Although the laptop's primary function was defined by the Respondent's employer to be the facilitation of "education, research and business," the Court gave little consideration to the work-related function of the laptop and to the employer's need for access. It also did not view the laptop as one part of an integrated information system intended to support work.

3. The Canadian Association of Counsel to Employers ("CACE") asks this Court to re-balance employer and employee interests. To strike a proper balance, the Court should give significant weight to the primary function of a work-issued computer and should recognize that a work-issued computer is only one part of a work information system that must be routinely accessed by an employer for a variety of legitimate reasons.

PART II – CONCISE STATEMENT OF POSITION

4. CACE takes no position on whether the Court should find an expectation of privacy in the circumstances. If this Court does find an expectation of privacy, CACE asks it to articulate a broad and clear corresponding right of employer access that will account for the intended function of a work computer and its information system and that will fully account for employers' need for unimpeded system access.

PART III – STATEMENT OF ARGUMENT

5. The Court's full consideration of the following four points is essential to the proper resolution of the appeal:

(a) A work information system is made up of a network of computers. Computers issued to employees are part of the network and need to be governed as part of the network.

(b) A work information system is a critical component of an employer's business infrastructure. Its function is to enable employees to communicate with each other in the course of work, to communicate externally in the course of work and to engage in productive work.

(c) A work information system is a repository of information about virtually all the activities of an organization – its communications, its transactions and its intellectual property. Employers must control the information on their systems and keep it secure.

(d) The value of information stored on a work information system to employers depends on access for a range of important purposes.

6. Below, we make argument on CACE's behalf with reference to these four points.

A) A work computer is part of a system and not a personal storage device

7. The Court of Appeal for Ontario erroneously viewed the laptop as a *segregated physical thing* intended to secure information from others, including the Respondent's employer. It said the Respondent had "exclusive possession" of the laptop (paras 36). It remarked that the laptop could be taken home on evenings, weekends and vacations and that it had a password "to exclude others" (para 45). The Court made its physical conception most clear by comparing the laptop to the storage locker considered by this Court in *R v Buhay* (para 42).

Reasons for Judgement, Court of Appeal, March 22, 2011, *Appellant's Record, Vol I* at paras 36, 42, 45.

8. *Buhay* is about the reasonable expectation of privacy associated with things placed in a public storage locker. This Court unanimously found an expectation of privacy. Arbour J, for the Court, said, "Indeed, generally, the purpose for renting a locker in such a location is to secure one's belongings against theft, damage, or even the simple curiosity of others." In this context, she explained that a locker owner's ability to gain access does not render a locker renter's expectation of privacy unreasonable.

R v Buhay, 2003 SCC 30 at paras 21, 22, [2003] 1 SCR 660, Arbour J.

9. Whatever personal information the Respondent stored on his laptop, he stored it side-by-side with "work product" that he generated in the course of employment, for his employer and in which he had a limited interest and could expect little or no privacy (*Phillips*). The *Buhay* analogy fails because the Respondent's employer had shared use of the laptop and an equal interest in securing the contents of the laptop. To employ the analogy correctly, the laptop was like a storage locker owned by the board and used by the board that contained *both the board and the Respondent's things.*

Evidence of R Taggart, *Appellant's Record, Vol I*, p 126, ll 12-17.

Exhibit E – Letter from D Smith to B Bourget, *Appellant's Record, Vol II*, p 220 (second last para).

Phillips v Vancouver Sun, 2004 BCCA 14 at para. 90, (2004) 238 DLR (4th) 167, Prowse J [*Phillips*].

10. The Respondent also stored his personal information on a device that he needed to connect to a network of other board-owned computers to do his work. In this mode, the Respondent could expect little privacy. The board did not need a password to access the Respondent's laptop when it was connected to its network. More significantly, the record shows that the Respondent's password was a means used by the board to reliably identify his network activity and to control his network access *for its own purposes*. For example:

(a) The board's acceptable use policy required users to log in using their assigned identity.

(b) A board technician testified that user accounts are "authenticated" and testified to observing activity "from Richard's machine" that led him to find the information that became the subject of criminal charges.

(c) The Respondent's principal testified that the board granted the Respondent special "domain admin rights" – described as allowing the Respondent broader access to information on its network and the right to set privileges for other users.

The password was a means of allowing for reliable identification that weighed against Respondent's privacy, though the Court of Appeal for Ontario considered the password in reaching the opposite conclusion.

> Exhibit A – Policy and Procedure Manual, P9.06, *Appellant's Record, Vol II*, p 175 (under the heading "identity").
>
> Evidence of R Taggart, *Appellant's Record, Vol I*, p 127, ll 7-8 (authentication) and p 132, ll 26, 27 ("Richard's machine").
>
> Evidence of B Bourget, *Appellant's Record, Vol II*, pp 10, l 21 - p 11, l 19.

B) A work information system serves a critical business function

11. The laptop was part of a work information system that had an important *primary* function - to enable employees to communicate with each other in the course of work, to communicate externally in the course of work and to engage in productive work. If the function of a work information system is acknowledged, (a) personal use is rightly-framed as a convenience that is not worthy of constitutional protection and (b) personal information that an employee chooses to intermingle with work information should not govern the expectation of privacy.

> Exhibit A – Policy and Procedure Manual, P9.06, *Appellant's Record, Vol II*, pp 174, 175.

12. Personal use of a work system is, by its very nature, secondary and a privilege – a convenience to employees and an alternative to using a home computer or a personally-owned device. Ensuring this convenience is available to employees in our society is not required to support the values of "dignity, integrity and autonomy" that underlie section 8 (see *Godoy*). The personal choice at issue in this matter is not like the choice with whom to associate and communicate that was protected by this Court in *R v Duarte* nor is it like the choice to meet in spaces accessible to the public protected in *R v Wong*. A decision in this matter that causes employees to be circumspect about what they choose to send, receive and store on their employers' work systems will not offend the values underlying section 8, yet it will pay proper respect to employers' important competing interest.

> *R v Godoy*, [1999] 1 SCR 311 at para 19, Lamer CJ [*Godoy*].
>
> *R v Duarte*, [1990] 1 SCR 30 at p 51e, LaForest J.
>
> *R v Wong*, [1990] 3 SCR 36 at p 52i, LaForest J.

13. The Respondent (paras 23 - 28, RF) gives no consideration to employers' important competing interest or the function of a work computer in suggesting that a work computer is perfectly analogous to a personally-owned computer. He suggests that computers – whatever use to which they are put – are meant to store "virtually every aspect of one's private life" (para 25, RF).

14. CACE agrees that examining the content of a home computer or personally-owned device is highly intrusive, but a work computer is different because of its function. The very principled statements made by this Court in *R v Morelli* that the Respondent quotes (paras 24, 25, RF) underscore that employees have a *Charter*-protected alternative to personal use of a work computer.

15. The reasonable employee understands that there is a consequence to intermingling work product and personal information, takes advantage of the convenience of personal use for less sensitive personal computing needs and uses a home computer or personally-owned device before doing what needs to be kept private. Even if this Court accepts the

Respondent's assertion that employees today work long hours (paras 34-36, RF), putting employees to this choice is acceptable in a free and democratic society because it allows for individual control over the use and dissemination of personal information (*Mills*, *Westin*).

> *R v Mills*, [1999] 3 SCR 668 at paras 80, 81, McLachlin and Iacobucci JJ [*Mills*].
>
> Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7, 26 [*Westin*].

16. This is not a choice the Respondent made well. Assuming the pictures he stored of his wife contained nudity or were pornographic, the Respondent cannot represent the reasonable employee because storing such pictures on a work system is universally prohibited by employers (*e.g.* Exhibit A). The reasonable employee both follows the rules and is more discrete using his employer's system.

> See *e.g.* Exhibit A – Policy and Procedure Manual, P9.06, *Appellant's Record, Vol II*, 175. 176 (under "inappropriate content" headings).

17. In summary, the Respondent's position goes too far. He is right that computers have the capacity to store information that lies close to the "biographical core" (paras 38-31, RF), but his argument elevates convenient use of employer-maintained, confidential computing services to a constitutional imperative. This is wrong.

C) A work information system is a repository of information that must be secured

18. A reasonable employee ought to expect his employer to engage in network monitoring and similar security measures even in the absence of "clear and unambiguous" policy language given the kind of information that is stored on a work information system.

19. A work information system is a repository of information about virtually all the activity of an organization – its communications, its transactions, its intellectual property as well as information about others for whom it has custodial duties under privacy legislation. Employers have a legitimate interest in keeping such information secure that is oftentimes

backed by statutory duties (*e.g. MFIPPA*, see *Poliquin, Westin*). The Respondent's employer did so through network monitoring.

> *Municipal Freedom of Information and Protection of Privacy Act*, RRO 1990, Regulation 823, s 3 [*MFIPPA*].
>
> *Poliquin v Devon Canada Corporation*, 2009 ABCA 216 at 48, 454 AR 61, Fraser CJ [*Poliquin*].
>
> Westin, *supra* at 43.

20. Network monitoring is significant because computer misconduct generally does not happen through discernible physical action. People sit at computers to take information from employers – literally by the flick of a keystroke. People sit at computers when they download software from un-trustworthy sources that may be laden with viruses. This makes computer-related misconduct difficult to detect unless individuals use electronic means to "keep an eye out for things that are going wrong" – exactly what the board technologist who discovered the Respondent's activity said he was hired to do.

> Evidence of R Taggart, *Appellant's Record, Vol I*, p 126, ll 26-29.

21. This technologist discovered the Respondent's activity in conducting a scan of network activity "to protect the network" from threats and testified that he had previously discovered software on the Respondent's computer after doing a network search on the word "hack." Nonetheless, the Court of Appeal for Ontario characterized his actions as legitimate "maintenance" (para 58) at the same time making a point that "there was no evidence that anyone monitored or policed the teachers' use of their laptops" (para 41).

> Evidence of R Taggart, *Appellant's Record, Vol I*, p 130, ll 1,2 and p 135, ll 17-22.
>
> Reasons for Judgement, Court of Appeal, March 22, 2011, *Appellant's Record, Vol I* at paras 41, 58.

22. CACE agrees with the Court of Appeal for Ontario that the technician's activity was legitimate. However, that activity was as much about computer security as it was about maintenance, and the Court of Appeal for Ontario's narrow framing of the facts supports an

expectation of privacy in a manner that cannot be justified. The technician was engaged in network monitoring, a legitimate activity rooted in his duly diligent employer's interest in maintaining a secure information system. It was an activity that the Respondent and other board employees ought to have expected notwithstanding their personal use.

D) Employers need a broad and clear right of access to information on their systems

23. The function of a work information system will be undermined if an employee expectation of privacy is recognized without also recognizing a broad and clear right of access. Such a right must allow employers to gain access to information on their systems for all legitimate purposes without fear of becoming engaged in a workplace dispute.

24. The Court of Appeal for Ontario does acknowledge the need for an implied management right. Having recognized an expectation of privacy, it recognizes a corresponding right to access information stored on a corporate information system "for the limited purpose of maintaining [the system's] technical integrity" (para 58). The Court's intention is well-founded, but its implied right is so narrow that, in the whole, its judgement is likely to preclude employers from using their work systems as designed.

> Reasons for Judgement, Court of Appeal, March 22, 2011, *Appellant's Record, Vol I* at paras 45, 58.

25. Consider the following common scenarios, all of which fall outside of the Court of Appeal for Ontario's recognized right:

(a) An employee is overcome by sudden illness. An employer searches the employee's laptop for work product that can be provided to the employee who is taking over the absent employee's duties.

(b) An employer has completed a multi-million dollar software development project and has hired a consultant to conduct a project debrief and make recommendations for the management of future projects. The consultant interviews

team members but also wishes to study the record of e-mail and text message communications sent over the employer's network.

(c) An employer must produce all e-mails related to its defence of a civil action. It retrieves whole e-mail accounts and searches them for relevant e-mails because centralized processing is efficient and defensible.

(d) An employer receives a printout of sexually harassing e-mail sent by one employee to another. The employer reviews the sender's e-mail account to determine if this is one incident of many. In the course of the ensuing investigation, the respondent employee denies sending the e-mail and there is no circumstantial evidence to show otherwise. As a result, the employer hires an IT forensics professional to examine the hard drive of the respondent employee's computer.

26. These four scenarios are all amenable to judicial notice (*Find*) and illustrate that employers require system access for a variety of important and legitimate purposes. The first two scenarios are rooted in an employer's private interest in operating efficiently but are legitimate nonetheless. The third scenario supports the public interest in the efficient administration of justice. The last scenario raises employer duties under anti-discrimination legislation that this Court has stressed are very strict because employers *control their workplaces* and "are in a position to take effective remedial action to remove undesirable conditions" (*Robichaud*, see also *Poliquin*).

> *R v Find*, 2001 SCC 32 at para 48, [2001] 1 SCR 863, McLachlin CJ [*Find*].
>
> *Robichaud v Canada (Treasury Board)*, [1987] 2 SCR 84 at p 95a, LaForest J [*Robichaud*].
>
> *Poliquin, supra* at paras 46, 47.

27. The decision appealed from creates a risk to employers' control of their workplaces and creates a real potential for conflict with employees by suggesting that the legitimate and important activities that we have outlined above must be set out in "clear and

unambiguous" policy to be authorized. CACE agrees that clear and unambiguous policy is an ideal. Such language should not be a necessity, however, because the need for employer access is fundamental. It is based on the function of a work computer and employers' right and responsibility to govern their workplaces.

28. In light of the above, should the Court recognize that the Respondent had an expectation of privacy in the content of his work-issued computer, CACE asks it to also recognize that employers have a right to access their work systems:

(a) to engage in technical maintenance, repair and management;

(b) to meet a legal requirement to produce, including by engaging in e-discovery;

(c) to ensure continuity of work processes;

(d) to improve business processes and manage productivity; and

(e) to prevent misconduct and ensure compliance with the law.

29. If an employee, in the circumstances, has a reasonable expectation of privacy in information stored on a work computer notwithstanding the function of the computer and the employer's interest in the proper functioning of its work information system, an employer should still have unimpeded access to the information if its actions are reasonably related to one or more of these five legitimate purposes.

PART V – REQUEST TO MAKE ORAL ARGUMENT

30. CACE requests permission to present oral argument for no more than 10 minutes.

All of which is respectfully submitted by Counsel for the Intervener CACE:

Daniel Michaluk

Joseph Cohen-Lyons

PART VI – TABLE OF AUTHORITIES

Tab	Jurisprudence	Pages/Paras
1	*R v Buhay*, 2003 SCC 30, [2003] 1 SCR 660, Arbour J.	paras 21, 22
2	*R v Duarte*, [1990] 1 SCR 30, Laforest J.	p 51e
3	*R v Find*, 2001 SCC 32, [2001] 1 SCR 863, McLachlin CJ.	para 48
4	*R v Godoy*, [1999] 1 SCR 311, Lamer CJ.	para 19
	R v Mills, [1999] 3 SCR 668, McLachlin and Iacobucci JJ.	paras 80, 81
5	*Robichaud v Canada (Treasury Board)*, [1987] 2 SCR 84, LaForest J.	p 95a
6	*Phillips v Vancouver Sun*, 2004 BCCA 14, (2004) 238 DLR (4th) 167, Prowse J.	para 90
7	*Poliquin v Devon Canada Corporation*, 2009 ABCA 216, 454 AR 61, Fraser CJ.	paras 45-49
8	*R v Wong*, [1990] 3 SCR 36, Laforest J.	p 52i
	Secondary Sources	
9	Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967)	pp 7, 26, 43

PART VII – STATUES, REGULATIONS AND RULES

1. *Municipal Freedom of Information and Protection of Privacy Act*, RRO 1990, Regulation 823, s 3.

3. (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

(2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.

(3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.