

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

BETWEEN:

HER MAJESTY THE QUEEN

**APPELLANT
(Respondent)**

and

RICHARD COLE

**RESPONDENT
(Applicant/Appellant)**

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

**FACTUM OF THE INTERVENER
THE DIRECTOR OF PUBLIC PROSECUTIONS
(Pursuant to Rules 37 and 42 of the *Rules of the Supreme Court of Canada*)**

Public Prosecution Service of Canada
Alberta Regional Office (Edmonton)
EPCOR Tower
700, 10423 – 101 Street
Edmonton, Alberta T5H 0E7
(Per: Ronald C. Reimer and
Monique B. Dion)
Telephone: (780) 495-4079
Fax: (780) 495-6940
Email: ron.reimer@ppsc-sppc.gc.ca)

Counsel for the Intervener

Brian Saunders
Director of Public Prosecutions
East Memorial Building, 2nd Floor
284 Wellington Street
Ottawa, Ontario
K1A 0H8
(Per: François Lacasse)
Telephone: (613) 957-4770
Fax: (613) 941-7865
Email: flacasse@ppsc-sppc.gc.ca

Ottawa Agent for the Intervener

Amy Alyea
Frank Au
Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, Ontario
M5G 2K1

Telephone: (416) 326-4600
Fax: (416) 326-4656
Email: amy.alyea@ontario.ca

Counsel for The Appellant

Frank Addario
Addario Law Group
171 John Street, Suite 101
Toronto, Ontario
M5T 1X3

Telephone: (416) 979-6446
Fax: (866) 714-1196
Email: faddario@addario.ca

Counsel for the Respondent,
Richard Cole

Gerald Chan
Nader R. Hasan
Ruby Shiller Chan, Barristers
11 Prince Arthur Avenue
Toronto, Ontario
M5R 1B2

Telephone: (416) 964-9664
Fax: (416) 964-8305

Counsel for the Respondent,
Richard Cole

Robert E. Houston, Q.C.
Burke-Robertson
Barristers & Solicitors
70 Gloucester Street
Ottawa, Ontario
K2P 0A2

Telephone: (613) 566-2058
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Ottawa Agent for the Appellant

Colleen Bauman
Sack Goldblatt Mitchell LLP
30 Metcalfe Street, Suite 500
Ottawa, Ontario
K1P 5L4

Telephone: (613) 235-5327
Fax: (613) 235-3014
Email: cbauman@sgmlaw.com

Ottawa Agent for the Respondent,
Richard Cole

Jonathan Dawe
Michael Dineen
Dawe & Dineen
171 John Street, Suite 101
Toronto, Ontario
M5T 1X3

Telephone: (416) 649-5058
Fax: (416) 352-7733
Email: jdawe@dawedineen.com

Counsel for the Intervener
Criminal Lawyers' Association (Ontario)

Jonathan C. Lisus
Michael Perlin
Lax O'Sullivan Scott Lisus LLP
145 King Street West
Suite 1920
Toronto, Ontario
M5H 1J8

Telephone: (416) 598-1744
Fax: (416) 598-3730
Email: jliskus@counsel-toronto.com

Counsel for the Intervener
Canadian Civil Liberties Association

Daniel Michaluk
Hicks Morley Hamilton Stewart Storie LLP
77 King Street West, 39th Floor
Box 371, TD Centre
Toronto, Ontario
M5H 1K8

Telephone: (416) 864-7253
Fax: (416) 362-9680
Email: daniel-michaluk@hicksmorley.com

Counsel for the Intervener,
Canadian Association of Counsel to
Employers

Ed Van Bemmell
Gowling Lafleur Henderson LLP
160 Elgin Street
Suite 2600
Ottawa, Ontario
K1P 1C3

Telephone: (613) 233-1781
Fax: (613) 563-9869
Email: ed.vanbemmell@gowlings.com

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

Henry S. Brown, Q.C.
Gowling Lafleur Henderson LLP
Barristers & Solicitors
160 Elgin Street
Suite 2600
Ottawa, Ontario
K1P 1C3

Telephone: (613) 233-1781
Fax: (613) 563-9869
Email: henry.brown@gowlings.com

Ottawa Agent for the Intervener,
Canadian Civil Liberties Association

Siobhan O'Brien
Hicks Morley Hamilton Stewart Storie LLP
150 Metcalfe Street
Suite 2000
Ottawa, Ontario
K2P 1P1

Telephone: (613) 369-8411
Fax: (613) 234-0418
Email: siobhan-obrien@hicksmorley.com

Agent for the Intervener,
Canadian Association of Counsel to
Employers

Dominique A. Jobin
Procureur général du Québec
1200, route de l'Église, 2e étage
Sainte-Foy, Québec
G1V 4M1

Téléphone: (418) 643-1477, ex. 20788
Télécopieur: (418) 644-7030
Email: djobin@justice.gouv.qc.ca

Counsel for the Intervener,
Attorney General of Quebec

Pierre Landry
Noël & Associés
111, rue Champlain
Gatineau, Québec
J8X 3R1

Téléphone: (819) 771-7393
Télécopieur: (819) 771-5397
Email: p.landry@noelassociés.com

Ottawa Agent for the Intervener,
Attorney General of Quebec

Table of Contents

	Page Number
PART I A. OVERVIEW STATEMENT	1
B. STATEMENT OF FACTS	1
PART II ISSUES	1
PART III ARGUMENT	1
PART IV COSTS	10
PART V REQUEST TO MAKE ORAL ARGUMENT	10
PART VI TABLE OF AUTHORITIES	11
PART VII STATUTES, REGULATIONS AND RULES	15
<i>Canadian Charter of Rights and Freedoms, Section 8</i>	15
<i>Access to Information Act, R.S., 1985, c. A-1, s. 4</i>	15

PART I - A. OVERVIEW STATEMENT

1. Section 8 of the *Charter* is not abridged by employment-related monitoring of a government employee's use of employer-issued computer equipment, particularly when the employee has been warned that such monitoring may occur. Assuming such monitoring engages s. 8 of the *Charter* and involves a "search," that "search" cannot be regarded as unreasonable. All employers require the ability, for employment-related purposes, to intrude upon their employees' limited privacy interest in data stored upon a work computer. The imposition of a warrant requirement or other exacting constitutional standard would unduly infringe the government's legitimate interest in effective management of the workplace.

PART I - B. STATEMENT OF FACTS

2. The Director of Public Prosecutions accepts the facts as stated by the parties and takes no position on any factual disputes between the parties. The salient facts relative to this submission are that data on an employer-issued computer was reviewed by an employer for work-related purposes as the employee had been warned might happen.

PART II - ISSUES

3. The Director of Public Prosecutions intervenes to address the question of whether an employer's review of data on a work-issued computer, if it be a "search" under s. 8 of the *Charter* when undertaken for legitimate employment-related purposes, should be regarded as unreasonable.

PART III - ARGUMENT

4. As the appellant has argued, an employee such as the respondent has no objectively reasonable expectation of privacy against his employer's review of data on a work-issued computer. But if this Court were to conclude that such employer actions involve a "search" then this Court should nonetheless conclude that it is a reasonable search.

5. Employers, including government employers, must have broad powers to conduct surveillance of the workplace and to monitor the use of employer-issued property and equipment. The fact that network-computing and the internet are now commonplace features of the workplace presents formidable challenges for all employers. Many employers consider it essential to monitor employee use of computer equipment and networks to preserve the integrity and efficacy of employers' computing systems, to ensure productivity and prevent abuses of, or illegal use of, the internet, and to manage the potential legal impacts of communications transmitted by employees.¹ Subject to a conflicting statutory or contractual obligation to safeguard employee privacy, the special needs of the government as employer make reasonable any "search" of data on a government-issued computer undertaken for any legitimate work-related purpose, including disciplinary matters. A constitutional challenge of this practice has even less merit, when the employer has also warned its employees that such monitoring may occur.

6. Any expectations of privacy that employees retain at work must be balanced against the legitimate needs of employers to protect their own property and to supervise and manage the workplace. This Court should not lose sight of the fact that the sole reason an employer provides an employee with office space or equipment, such as an unshared laptop computer, is to facilitate the employee's performance of his work for that employer. In this sense, a work computer must be regarded as an extension of the workplace. Mere recognition by the employer that an employee may choose to keep some personal items in her office or some personal data on her employer-issued computer does not detract from the understanding of all concerned that the office space or electronic device will be used primarily for work related purposes. And it is no basis for concluding that the employer has surrendered access to its offices or computers by assigning a specific office space or a particular electronic device to an employee.

7. In this case, the reasonable law that authorizes such workplace "searches" is the common law of employment in Canada. Broad power to conduct surveillance and monitor workers for legitimate employment-related reasons has been widely accepted by

¹ Michael A. Geist, "Computer and E-mail Workplace Surveillance in Canada" (2003) 82 C.B.R. 153 [Geist] "Up to 14 million workers in the United States alone have their e-mail and Internet use monitored . A 2001 survey by the American Management Association (AMA) revealed that nearly 80 percent of major U.S. companies monitor employee e-mail and Internet use..."

Canadian courts and arbitration boards both in the private sector, where *Charter* values influence the development of the common law and in the public sector, where the *Charter* has direct application.

8. In the private sector, the vast weight of Canadian authority upholds the right of employers to utilize surveillance of all kinds² and more specifically monitoring of employee use of computers and computer networks to manage the workplace. And whether those management rights flow from the common law or are stated in collective agreements, they have been widely accepted as sufficient authority to intrude upon employee privacy in the workplace absent any countervailing employee-privacy contractual or statutory obligations. Employers are generally entitled to conduct surveillance in their premises and in respect of their equipment, including computer equipment and networks.³ Where, as here, the employees have also been warned that such monitoring may occur, that circumstance has been held to be conclusive of the legitimacy of such monitoring, except in circumstances where the monitoring was needlessly intrusive or not sufficiently related to a valid management purpose.⁴

9. In public sector employment law, where *Charter* guarantees have direct application, work-related surveillance conducted by government employers has likewise been judged reasonable when done for valid management purposes and with advance

² See for example: *New Flyer Industries Ltd. v. CAW-Canada, Local 3003* (2000), 85 L.A.C. (4th) 304 (Manitoba Grievance Arbitration); *Kimberly-Clark Inc. v. I.W.A. – Canada, Local 1-92-4* (1996), 66 L.A.C. (4th) 266 (ON Arbitration Board); *Canadian Timken Ltd. v. U.S.W.A., Local 4906* (2001), 98 L.A.C. (4th) 129 (ON Arbitration Board) - surveillance of employees on sick leave/disability.

³ See for example: *Milsom v Corporate Computers Inc.*, 2003 ABQB 296; *Owens-Corning Canada Inc. v. Communications, Energy and Paperworkers Union of Canada, Local 728*, [2002] A.G.A.A. No. 74 (Alberta Grievance Arbitrator); *Naylor Publications Co. (Canada) v. Media Union of Manitoba, Local 191*, [2003] M.G.A.D. No. 21 (Manitoba Grievance Arbitration); *Lethbridge College v. Lethbridge College Faculty Assn.*, [2008] A.W.L.D. 1043 (Alberta Arbitration Board); *Re: Langley Cruiseshipcentres Ltd.* [2006] B.C.I.P.C.D. No. 39 (British Columbia Information and Privacy Commissioner) [*Langley*]; *Poliquin v. Devon Canada Corp.*, 2009 ABCA 216 [*Poliquin*] – improper use of email or internet.

⁴ *Cascade Aerospace Inc. v. CAW-Canada, Local 114* (2009), 186 L.A.C. (4th) 26 (Canada Arbitration Board) - decision to install a hidden camera to investigate vandalism/theft from a vending machine was found to be reasonable, however the camera was carelessly installed such that it also viewed employee private activity and therefore was in violation of *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; *Fraser Surrey Docks Ltd. v. I.L.W.U., Local 514* (2007), 159 L.A.C. (4th) 72 (Canada Arbitration Board) - focussed surveillance of a gas tank was reasonable as it had been initiated in response to concerns about theft of gas and was in an area subject to general surveillance; *Fraser Health Authority v. H.S.A.B.C.* (2011) 208 L.A.C. (4th) 107 (British Columbia Arbitration Board) - audit of employee's internet usage was upheld in the context of complaints by coworkers.

warning to employees that the specific type of monitoring or surveillance may be undertaken.⁵

10. Beyond the general need for monitoring and surveillance to effectively manage the workplace, employers face strenuous challenges in preserving the integrity and efficacy of their computing systems. Personal computer usage such as streaming video or audio and personal email containing large attachments can “clog a company’s telecommunications system.”⁶ Networked devices and computer networks are frequently the targets of electronic attacks to steal information or distribute “viruses” “worms” and other malicious software. Excluding personal information of employees from monitoring would logically present a distinct vulnerability. Employees who use their work computers for personal purposes pose no lesser threat to the network’s integrity.⁷ Malicious software has been introduced into institutional networks from personal as opposed to work-related e-mails.⁸ Likewise, software, add-on devices, and zip drives installed by employees themselves likely pose a greater risk than those inspected and approved by the employer’s IT department.⁹

11. There can be no convenient water-tight compartmentalization of private versus workplace data; an employee’s use of the employer’s computer facilities for personal purposes routinely has legal impacts upon the employer itself. Documents created by a government employee for her own use may in some circumstances constitute public

⁵ See for example: *A.T.U. Local 569 v. Edmonton (City)*, 2004 ABQB 280; *O.L.B.E.U. v. Ontario (Liquor Control Board)*, (2005) 137 L.A.C. (4th) 350, (Ontario Crown Employees Grievance Settlement Board); *Toronto Transit Commission v. Amalgamated Transit Union, Local 113* (1999), 95 L.A.C. (4th) 402 (Ontario Arbitration Board) surveillance of public employees on sick leave.

See also: *Health Employer’s Association of British Columbia v. Health Science Association of British Columbia (Internet Audit Grievance)*, [2011] B.C.C.A.A.A. No. 60; *Briar v. Canada (Treasury Board)*, 2003 CarswellNat 3250 (PSSRB) [*Briar*]; and *Andrews v. Canada (Deputy Head - Department of Citizenship & Immigration)*, 2011 CarswellNat 3564 (CPSLRB) [*Andrews*] - audits of government employee’s email/internet.

⁶ *Geist*, *supra* note 1 at 156-157.

⁷ See for example: Noah Shachtman “Military May Ban Twitter, Facebook as Security ‘Headaches’” *Wired* (30 July 2009) online: <http://www.wired.com/dangerroom/2009/07/military-may-ban-twitter-facebook-as-security-headaches/>

⁸ ILOVEYOU virus, infected 45 million computers and was estimated to cause 1 billion dollars in damages. Mark Ward “A decade on from the ILOVEYOU bug” *BBC News* (4 May 2010) online: <http://www.bbc.co.uk/news/10095957>; D. Ian Hopper “ILOVEYOU’ computer bug bites hard, spreads fast” *CNN* (May 4, 2000) online: http://articles.cnn.com/2000-05-04/tech/iloveyou.01_1_melissa-virus-antivirus-companies-iloveyou-virus?_s=PM:TECH.

⁹ See for example: Noah Shachtman “Under Worm Assault, Military Bans Disks, USB Drives” *Wired* (19 November 2008) online: <http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/>.

records that the government agency is obliged to preserve and make available to the public under Access to Information legislation.¹⁰ Employees sometimes discuss, in personal emails, sensitive work-related matters in which an employer may have proprietary interests or other compelling reasons for keeping confidential.¹¹ When confronted with claims of negligence or wrongful dismissal, an employee's personal documents may be relevant discovery material essential to assessing or defending the employer's litigation position.¹² Employers also have a distinct interest in preventing and detecting a hostile work environment¹³ and access to an employee's personal emails distributed using the employer's network is essential to root out cases of harassment and cyber-bullying.¹⁴ These examples show that employers have a valid interest in monitoring not only the electronic health of their networks but the contents of employee communications transmitted over the employer's equipment or stored in its hard drives.

12. The potential for abuse of internet privileges is another good reason why employers monitor the use of their computer networks. Many employers find it necessary and effective to provide their employees with access to the internet for business purposes. But providing access to the internet carries distinct risks that employees will waste work time visiting social-networking sites, shopping on-line, viewing legal pornography, studying on internet campuses or watching professional sports, to name but a few examples from the virtual world of tempting and time-consuming activities that are on

¹⁰ *Access to Information Act*, R.S.C., 1985, c. A-1 s. 4.

¹¹ *Geist*, supra note 1 at 158 – "Fortune 1000 companies sustained losses of more than \$45 billion in 1999 from the theft of proprietary information." For Canadian cases see: *Nesbitt Burns Inc. v. Lange*, 2000 Carswell Ont 1296 (ONSCJ); *Langley*, supra note 3.

¹² *Lovelock v. Dupont Canada Inc.*, [1998] O.J. No. 4971 (ONCJGD) an action for wrongful dismissal where the employer relied on an email sent by the employee to rebut the employees contentions; *Pacific Northwest Herb Corp. v. Thompson*, [1999] B.C.J. No. 2772 (BCSC) where in a similar action the court substantially denied an application for an injunction by the employee to prevent the employer from having access to an employer owned laptop which may have contained business records that were relevant to the action.

¹³ Indeed there is a legal obligation to prevent discriminatory practices such as sexual harassment, as noted by the Intervener Canadian Association of Counsel to Employers at para. 26 of its factum.

¹⁴ *Di Vito v. MacDonald Dettwiler & Associates Ltd.*, [1996] B.C.L.R.D. 2036 - employee circulated an email regarding co-worker's weight problems and a recipient posted it to the company bulletin board. See also: *Poliquin*, supra note 3 at para 46 where the Alberta Court of Appeal stated that racist and pornographic emails can "easily poison a work environment."

offer twenty-four hours a day.¹⁵ And, government and other large institutional employers have a distinct interest beyond concerns about office efficiency for ensuring that their employees are using the internet in an appropriate manner. The internet also presents a world of inappropriate material such as child pornography, discriminatory comedy and extremist political invective.¹⁶ Abuse of employer-issued equipment and internet privileges to view material that is illegal, or even distasteful, is unacceptable to taxpayers and shareholders alike and risks associating a corporation or government organization with actions and ideas fundamentally inconsistent with its values and ethics.¹⁷ In addition, when such malfeasance occurs at a government agency with direct responsibility for investigating or enforcing the law, the reflection on the employer is even more glaring.

13. This Court's context-specific approach to s. 8 of the *Charter* mandates consideration of these grave concerns because every government employer has at least all of the same important interests in effective management of the workplace and no fewer apprehensions about the effective and appropriate use of its computer resources as does any private employer. These special needs and the legitimate government goal of effective workplace management must, therefore, be balanced against any residual expectation of privacy that government employees may have in the workplace.

¹⁵ *Geist*, *supra* note 1 at 155-156: "Canadian employees waste nearly 800 million work hours each year surfing the [Internet] for personal reasons... ..Canadians with Internet access at work spend an average of eight hours on-line a week, and of that, at least two hours is spent on personal matters."

See for example: *Andrews*, *supra* note 5 at para. 11 - grievor terminated for excessive internet use admitted to spending 50-100% of his work time surfing internet sites unrelated to his employment.

¹⁶ As to inappropriate use generally see: *British Columbia v. B.C.G.E.U.*, 2010 CarswellBC 2843 (British Columbia Arbitration Board) where employee was dismissed for the distribution emails including hard core pornography that was offensive to women and other emails that were offensive to gay men and various ethnic groups; *Briar*, *supra* note 5 at para 22 - racist, misogynistic and homophobic emails distributed through the work email system, *O.P.S.E.U. v. Ontario (Ministry of Natural Resources)*, 2003 CarswellOnt 3343 (Ontario Crown Employees Grievance Settlement Board) - sexually violent images and bestiality.

¹⁷ See: *Poliquin*, *supra* note 3 at para 49 - "In the information technology world of today, email can be disseminated to many inside of an organization with the click of the mouse... ..this reality substantially increases the risk to employers flowing from the misuse of their equipment and Internet access for improper purposes." See also: employee disciplined for maintaining a blog depicting pro-Hitler and violent fantasies that identified employer (*EV Logistics v. Retail Wholesale Union, Local 580*, [2008] B.C.W.L.D. 2814 (BCLRB)) or a Facebook page that displayed negative stereotypes of aboriginal peoples (*S.G.E.U. v. Saskatchewan (Ministry of Corrections, Public Safety & Policing)*, 2009 CarswellSask 913 (Saskatchewan Arbitration Board)). Where employees disciplined for promulgating disparaging remarks about employer on a personal blog (*Alberta v. A.U.P.E.*, 2010 ABCA 216) or Facebook page (*Wasaya Airways LP v. Air Line Pilots Assn., International* (2010), 195 L.A.C. (4th) 1 (CLA) and *Loughheed Imports Ltd. v. U.F.C.W., Local 1518*, [2011] B.C.W.L.D. 318 (BCLRB)).

14. Recognition of the government's special needs to manage the workplace and to protect and control its computing resources is also entirely consistent with the principle, accepted by this Court in *New Brunswick v. Dunsmuir*, that the application of the *Charter* and other public-law obligations are attenuated when the government is acting as a private contracting party (under a contract of employment or collective agreement as in this case) rather than as sovereign applying rules and policies applicable to all of society.¹⁸

15. By contrast it is wholly unreasonable to suggest, as the respondent has done, that such monitoring by a government employer violates s. 8 in the absence of a warrant based upon reasonable grounds. There is no justification for importing these requirements, which are generally applied when an individual is singled out on suspicion of criminal activity by state agents responsible for law enforcement, into the employment context. The concepts of a search warrant and reasonable grounds to believe have no application to the kind of "searches" involved here which are simply part of the normal employer-employee relationship—a routine network maintenance review and a disciplinary investigation into compliance with an employer's acceptable-computer-use policy. It is simply unreasonable to render these everyday employment decisions constitutional matters subject to warrant requirements. Likewise, it is equally unreasonable to expect that government managers be required to master the nuances of police procedure such as what constitutes reasonable grounds to believe or an understanding of when it is permissible to search without a warrant. Beyond the monumental task of schooling the nation's middle-managers in the fine points of establishing a credibly-based probability, such a management-model would inevitably produce chaos in the workplace.

16. A review of this Court's s. 8 jurisprudence shows that the exacting constitutional standard of reasonable grounds to believe has only been insisted upon in the context of law enforcement searches directed at gathering evidence of crime. In a wide array of other situations, where the government's interest is different and the need to search mainly serves purposes apart from the investigation and prosecution of crime, this Court

¹⁸ *New Brunswick (Board of Management) v. Dunsmuir*, [2008] 1 S.C.R. 190 at para 81, 103-105; see also: *Air Canada v. Toronto Port Authority*, 2011 FCA 347 at para 52-53.

has judged reasonable other forms of justification more specifically tailored to the particular circumstances of an individual's interaction with the government. There are numerous examples that illustrate this principle. Regulatory inspections were judged reasonable in light of the diminished expectation of privacy in a closely-regulated activity and the societal interest in protecting public health and welfare.¹⁹ Likewise, it was held to be reasonable for government to demand retention and production of documents within regulated activities and in order to maintain a self-reporting system of taxation.²⁰ The government's interest in controlling the flow of goods and contraband across international boundaries was sufficient to overcome the privacy interest of international travellers in their personal belongings based only upon the reasonable suspicion of a Custom's official.²¹ The government's interest in improving the criminal justice system through better identification of criminals was held sufficient to outweigh the privacy interests of convicted criminals in the case of DNA data banking²² and of arrestees in the case of fingerprinting.²³ This Court has also accepted much reduced justification for searching in the case of those subject to imprisonment.²⁴ And notably, this Court fashioned a special model of search authority for school officials to address the special need to safeguard the school environment from contraband drugs and weapons.²⁵ In short, this Court's broader s. 8 teachings support the view that the assessment of whether a search is reasonable must always be context specific and must take account of the specific government goals that weigh against the individual interest in privacy.

17. In the workplace, the overarching reasonableness test embodied in s. 8 is satisfied if the employer's "search" is closely related to a management interest, including the employee's performance of work duties. This conclusion holds both when the employer makes benign entries (such as a computer technician's review of network electronic

¹⁹ *R. v. Fitzpatrick*, [1995] 4 S.C.R. 154 at 184-185; *Comité Paritaire de L'industrie de la Chemise v. Potash*; *Comité Paritaire de L'industrie de la Chemise v. Sélection Milton*, [1994] 2 S.C.R. 406 at 444-445; and *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425 [*Thomson Newspapers*] at 505-508.

²⁰ *Thomson Newspapers*, *supra* note 19 at 596-597; *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627 at 649-650; *Del Zotto v. Canada*, [1999] 1 S.C.R. 3 rev'g [1997] 3 F.C. 40; *R. v. Jarvis*, [2002] 3 S.C.R. 757 at 808-809.

²¹ *R. v. Monney*, [1999] 1 S.C.R. 652 at 675.

²² *R. v. Rodgers*, [2006] 1 S.C.R. 554 at 587.

²³ *R. v. Beare*; *R. v. Higgins*, [1988] 2 S.C.R. 387 at 407.

²⁴ *Weatherall v. Canada (Attorney General)*, [1993] 2 S.C.R. 872 at 877.

²⁵ *R. v. M.(M.R.)*, [1998] 3 S.C.R. 393 at 421.

health or routine audits of government data and electronic property) and when the entries are done for more substantive reasons such as to assess employee performance and policy-compliance, including when the employee is suspected of misconduct or dereliction of duty. As demonstrated by the weighty concerns described herein, it is imperative that employers have the means to manage and detect malfeasance in the cyber-workplace.

18. In that connection, it is simply unworkable to suggest as the Court of Appeal did in this case²⁶ that a computer technician informing and showing his discovery to a manager involved a separate search requiring that s. 8 be revisited. If systems monitoring by a technician does not offend s. 8, either because it does not involve a search or because it a reasonable search, then the act of sharing it with a supervisor does not engage s. 8. An employee simply cannot expect that discoveries of information with implications for discipline, made in the course of more benign and routine monitoring, will not be disclosed to persons with supervisory responsibilities. Both the technician and the manager are engaged in the work of the same employer.

19. When the employer has also forewarned employees that this kind of monitoring may occur, there is even less basis for challenging the reasonableness of the employer's review of data on a work-issued computer. Beyond the obvious fairness involved in that approach, it directly informs employee choices regarding sensitive personal cyber data. Employees may find it convenient and cost-effective to run their personal and professional lives from the work-computer, but they do not lack for better privacy alternatives. They can easily forego personal use of the work computer altogether or at least in respect of those personal activities that they wish to remain private. That may have seemed less practicable twenty years ago when computers were generally bulkier and more expensive, but today millions of Canadians conduct their personal cyber interactions using small portable wireless devices such as tablets and smart-phones. The fact that some employees may reject better privacy options for reasons of convenience, inertia or personal economy, is not sufficient reason to outweigh their employers' vital interest in effective management of the cyber workplace.

²⁶ *R. v. Cole*, 2011 ONCA 218 at para 60.

PART IV - COSTS

20. The Director of Public Prosecutions makes no submissions with respect to costs.

PART V - REQUEST TO MAKE ORAL ARGUMENT

21. The Director of Public Prosecutions requests permission to present oral argument at the hearing of the appeal.

ALL OF WHICH IS RESPECTFULLY SUBMITTED,

Ron Reimer



Monique Dion

Counsel for the Intervener,
Director of Public Prosecutions of Canada

30 April 2012

PART VI
TABLE OF AUTHORITIES

<u>TAB</u> <u>Cases Cited</u>	<u>Para.</u>
1. <i>Air Canada v. Toronto Port Authority</i> , 2011 FCA 347; A.C.W.S. (3d) 254	14
2. <i>Alberta v. A.U.P.E.</i> , 2010 ABCA 216; 482 A.R. 292 [EXCERPT ONLY : HN]	12
3. <i>Andrews v. Canada (Deputy Head - Department of Citizenship & Immigration)</i> , 2011 CarswellNat 3564 554; 2011 PSLRB100 [EXCERPT ONLY : HN + P. 6]	9, 12
4. <i>A.T.U. Local 569 v. Edmonton (City)</i> , 2004 ABQB 280; 356 A.R. 228 [EXCERPT ONLY : HN]	9
5. <i>Beare, R. v.; R. v. Higgins</i> , [1987] S.C.J. No. 92; [1988] 2 S.C.R. 387 [EXCERPT ONLY : HN + P. 407]	16
6. <i>Briar v. Canada (Treasury Board)</i> , 116 L.A.C. (4 th) 418, 2003 PSSRB 3	9, 12
7. <i>British Columbia v. B.C.G.E.U.</i> , 194 L.A.C. (4 th) 97, [2010] B.C.W.L.D. 8412 (British Columbia Arbitration Board)	12
8. <i>Canadian Timken Ltd. v. U.S.W.A., Local 4906 (2001)</i> , 98 L.A.C. (4 th) 129 2001 CarswellOnt 6010 (ON Arbitration Board); 2001 Carswell Ont. 6010	8
9. <i>Cascade Aerospace Inc. v. CAW-Canada, Local 114 (2009)</i> , 186 L.A.C. (4 th) 26 (Canada Arbitration Board); [2009] L.U.I. 3852-1	8
10. <i>Comité Paritaire de L'industrie de la Chemise v. Potash; Comité Paritaire de L'industrie de la Chemise v. Sélection Milton</i> , [1994] S.C.J. No. 7; [1994] 2 SCR 406 [EXCERPT ONLY : HN + PP. 444-445]	16
11. <i>Del Zotto v. Canada</i> , [1999] S.C.J. No. 1, [1999] 1 S.C.R. 3	16
12. <i>Del Zotto v. Canada</i> , [1997] 3 FC 40; [1997] A.C.F. no 795	16
13. <i>Di Vito v. MacDonald Dettwiler & Associates Ltd.</i> , [1996] B.C.L.R.D. 2036 554; 21 C.C.E.L. (2d) 137 [EXCERPT ONLY : HN]	11

14. ***(EV Logistics v. Retail Wholesale Union, Local 580***, [2008] B.C.W.L.D. 2814 (BCLRB)) 12
15. ***Fitzpatrick, R. v.***, [1995] S.C.J. No. 94; [1995] 4 SCR 154 16
[EXCERPT ONLY : HN + PP. 184-185]
16. ***Fraser Surrey Docks Ltd. v. I.L.W.U., Local 514 (2007)***, 159 L.A.C. (4th) 72 (Canada Arbitration Board); [2007] C.L.A.D. No. 48 8
17. ***Fraser Health Authority v. H.S.A.B.C.*** (2011) 208 L.A.C. (4th) 107 (British Columbia Arbitration Board); [2011] BCWLD 6162 [EXCERPT ONLY : HN] 8
18. ***Health Employer's Association of British Columbia v. Health Science Association of British Columbia (Internet Audit Grievance)***, [2011] B.C.C.A.A.A. No. 60; 208 L.A.C. (4th) 107 9
19. ***Jarvis, R. v.***, [2002] S.C.J. No. 76; [2002] 3 S.C.R. 757 16
[EXCERPT ONLY : HN + PP. 808-809]
20. ***Kimberly-Clark Inc. v. I.W.A. – Canada, Local 1-92-4 (1996)***, 66 L.A.C. (4th) 266, [1996] O.L.A.A. No. 46 (ON Arbitration Board) [EXCERPT ONLY : HN] 8
21. ***Lethbridge College v. Lethbridge College Faculty Assn.***, [2008] A.W.L.D. 1043, 166 L.A.C. (4th) 289 (Alberta Arbitration Board); 166 L.A.C. (4th) 289 8
22. ***Loughheed Imports Ltd. V. U.F.C.W., Local 1518***, [2011] B.C.W.L.D. 318 (BCLRB)); 186 C.L.R.B.R. (2d) 107 12
23. ***Lovelock v. Dupont Canada Inc.***, [1998] O.J. NO. 4971 (ONCJGD); 1998 Carswell Ont. 4626 11
24. ***McKinlay Transport Ltd., R. v.***, [1990] S.C.J. No. 25; [1990] 1 S.C.R. 627 [EXCERPT ONLY : HN + PP. 649-650] 16
25. ***Milsom v Corporate Computers Inc.***, 2003 ABQB 296, [2003] 9 W.W.R. 250; 17 Alta. L.R. (4th) 124 [EXCERPT ONLY : HN] 8
26. ***R. v. M.(M.R.)***, [1998] S.C.J. No. 83; [1998] 3 S.C.R. 393 16
[EXCERPT ONLY : HN + P. 421]

27. ***Monney, R. v.*** [1999] S.C.J. No. 18; [1999] 1 S.C.R. 652 16
[EXCERPT ONLY : HN + P. 675]
28. ***Naylor Publications Co. (Canada) v. Media Union of Manitoba, Local 191,*** [2003] M.G.A.D. No. 21 (Manitoba Grievance Arbitration) 8
29. ***Nesbitt Burns Inc. v. Lange,*** 2000 Carswell Ont 1296 (ONSCJ) 11
30. ***New Brunswick (Board of Management) v. Dunsmuir,*** 2008 SCC 9; [2008] 1 S.C.R. 190 [EXCERPT ONLY : HN + PP. 232 – 233, 241-242] 14
31. ***New Flyer Industries Ltd. v. CAW-Canada, Local 3003,*** 85 L.A.C. (4th) 304, 2000 CarswellMan 708 (Manitoba Grievance Arbitration); 2000 Carswell Man. 708 8
32. ***O.L.B.E.U. v. Ontario (Liquor Control Board),*** (2005) 137 L.A.C. (4th) 350, (Ontario Crown Employees Grievance Settlement Board); [2005] OGSBA No. 31 9
33. ***O.P.S.E.U. v. Ontario (Ministry of Natural Resources),*** 2003 CarswellOnt 3343 (Ontario Crown Employees Grievance Settlement Board); 115 L.A.C. (4th) 120 12
34. ***Owens-Corning Canada Inc. v. Communications, Energy and Paperworkers Union of Canada, Local 728,*** [2002] A.G.A.A. No. 74 , 113 L.A.C. (4th) 97 (Alberta Grievance Arbitrator) [EXCERPT ONLY : HN] 8
35. ***Pacific Northwest Herb Corp. v. Thompson,*** [1999] B.C.J. No. 2772 (BCSC); 1999 Carswell BC 2738 [EXCERPT ONLY : HN] 11
36. ***Poliquin v. Devon Canada Corp.,*** 2009 ABCA 216; 454 A.R. 61 [EXCERPT ONLY : HN + PP. 11-12] 8, 11, 12
37. ***Re: Langley Cruiseshipcentres Ltd.*** [2006] B.C.I.P.C.D. No. 39 (British Columbia Information and Privacy Commissioner) 8, 11
38. ***Rodgers, R. v.,*** [2006] S.C.J. No. 15; [2006] 1 S.C.R. 554 [EXCERPT ONLY : HN + PP. 586-587] 16
39. ***S.32G.E.U. v. Saskatchewan (Ministry of Corrections, Public Safety & Policing),*** 2009 CarswellSask 913 (Saskatchewan Arbitration Board) 12

40. ***Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)***, [1990] S.C.J. No. 23; [1990] 1 S.C.R. 425 [EXCERPT ONLY : HN + PP. 505-507, PP. 596 -597] 16
41. ***Toronto Transit Commission v. Amalgamated Transit Union, Local 113*** (1999), 95 L.A.C. (4th) 402 (Ontario Arbitration Board); [1999] OLAA No. 202 [EXCERPT ONLY : HN + PP. 3-4] 9
42. ***Wasaya Airways LP v. Air Line Pilots Assn., International*** (2010), 195 L.A.C. (4th) 1 (CLA) 554; [2010] C.L.A.D. No. 297 [EXCERPT ONLY : HN] 12
43. ***Weatherall v. Canada (Attorney General)***, [1993] S.C.J. No. 81; [1993] 2 S.C.R. 872 [EXCERPT ONLY : HN + PP. 876-877] 16

Other References

- Michael A. Geist, “Computer and E-mail Workplace Surveillance in Canada” (2003) 82 C.B.R. 153 (not reproduced, see Appellant’s Authorities, Volume I, Tab 8) 5, 10, 11, 12
44. D. Ian Hopper “‘ILOVEYOU’ Computer Bug Bites Hard, Spreads Fast” CNN (May 4, 2000) online: CNN <http://articles.cnn.com/2000-05-04/tech/iloveyou.01_1_melissa-virus-antivirus-companies-iloveyou-virus?s=PM:TECH>. 10
45. Noah Shachtman “Military May Ban Twitter, Facebook as Security ‘Headaches’” Wired (30 July 2009) online: Wired <<http://www.wired.com/dangerroom/2009/07/military-may-ban-twitter-facebook-as-security-headaches/>> 10
46. Noah Shachtman “Under Worm Assault, Military Bans Disks, USB Drives” Wired (19 November 2008) online: Wired <<http://www.wired.com/dangerroom/2008/11/army-bans-usb-d/>> 10
47. Mark Ward “A Decade on From the ILOVEYOU Bug” BBC News (4 May 2010) online: BBC News <<http://www.bbc.co.uk/news/10095957>> 10

PART VII
STATUTES, REGULATIONS AND RULES

Canadian Charter of Rights and Freedoms, Section 8

Everyone has the right to be secure against unreasonable search or seizure.

Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

Access to Information Act, R.S., 1985, c. A-1, s. 4

4. (1) Subject to this Act, but notwithstanding any other Act of Parliament, every person who is
(a) a Canadian citizen, or
(b) a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*,

has a right to and shall, on request, be given access to any record under the control of a government institution.

Extension of right by order

(2) The Governor in Council may, by order, extend the right to be given access to records under subsection (1) to include persons not referred to in that subsection and may set such conditions as the Governor in Council deems appropriate.

Responsibility of government institutions

(2.1) The head of a government institution shall, without regard to the identity of a person making a request for access to a record under the control of the institution, make every reasonable effort to assist the person in connection with the request, respond to the request accurately and

4. (1) Sous réserve des autres dispositions de la présente loi mais nonobstant toute autre loi fédérale, ont droit à l'accès aux documents relevant d'une institution fédérale et peuvent se les faire communiquer sur demande :
a) les citoyens canadiens;
b) les résidents permanents au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés*.

Extension par décret

(2) Le gouverneur en conseil peut, par décret, étendre, conditionnellement ou non, le droit d'accès visé au paragraphe (1) à des personnes autres que celles qui y sont mentionnées.

Responsable de l'institution fédérale

(2.1) Le responsable de l'institution fédérale fait tous les efforts raisonnables, sans égard à l'identité de la personne qui fait ou s'apprête à faire une demande, pour lui prêter toute l'assistance indiquée, donner suite à sa demande de façon précise et complète et, sous réserve des règlements, lui communiquer le document en temps

completely and, subject to the regulations, provide timely access to the record in the format requested.

Records produced from machine readable records

(3) For the purposes of this Act, any record requested under this Act that does not exist but can, subject to such limitations as may be prescribed by regulation, be produced from a machine readable record under the control of a government institution using computer hardware and software and technical expertise normally used by the government institution shall be deemed to be a record under the control of the government institution.

utile sur le support demandé.

Document issu d'un document informatisé

(3) Pour l'application de la présente loi, les documents qu'il est possible de préparer à partir d'un document informatisé relevant d'une institution fédérale sont eux-mêmes considérés comme relevant de celle-ci, même s'ils n'existent pas en tant que tels au moment où ils font l'objet d'une demande de communication. La présente disposition ne vaut que sous réserve des restrictions réglementaires éventuellement applicables à la possibilité de préparer les documents et que si l'institution a normalement à sa disposition le matériel, le logiciel et les compétences techniques nécessaires à la préparation.