# FREE SPEECH AND PRIVACY IN THE INTERNET AGE: THE CANADIAN PERSPECTIVE

> Gentlemen, progress has never been a bargain. You've got to pay for it. Sometimes I think there's a man behind the counter who says, "All right, you can have a telephone; but you'll have to give up privacy, the charm of distance. Madam, you may vote; but at a price; you lose the right to retreat behind a powder-puff or a petticoat. Mister, you may conquer the air; but the birds will lose their wonder, and the clouds will smell of gasoline!"
>
> Address to the jury by William Drummond, from
> *Inherit the Wind*, Act 2, Scene 2
> by J. Lawrence and R.E. Lee

Paula Knopf†

Arbitrators often have to balance competing interests. In the more challenging cases, there is validity and merit to the interests that must be balanced. The topic "Free Speech and Privacy in the Internet Age" raises many competing and valid interests. On the one hand, there is a need in the new era of information technology to be able to research and communicate with speed and ease. On the other hand, there is a need to ensure that the same technology does not invade personal privacy. Further, while employers have the right to control the use of their equipment and resources, employees still retain rights concerning their individual dignity. The immortal words of Greta Garbo can be heard by movie stars and employees alike: " I want to be alone." Yet if the Internet is, by definition a "worldwide system of interconnected computers,"[1] one has to also wonder whether privacy exists at all in this realm.

† Arbitrator, Mediator, and Adjunct Professor of Law at Osgoode Hall Law School, York University, Toronto, Canada.

1. Mark S. Dichter & Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, *at* http://www.morganlewis.com/pdfs/A5C845ED-575B-4ADC-8A47F2801DC3594C_Publication.pdf.

This paper is designed to look at the Canadian labor relations community's perspective on these interests. The media has recently reported a number of interesting cases that bring the topic to mind. For example, a highly ranked and decorated member of the Canadian military was demoted after revealing that he had used a military issued laptop, but his own private Internet account, to access a "soft" pornography Web site. He disclosed this when he was called upon to discipline a subordinate for alleged misuse of the military's e-mail system. The public outcry in the press, both for and against this officer, was intense. Some felt that it was ridiculous to discipline anyone for this, let alone a decorated member of our armed forces. Others felt that his accessing a pornographic site on a computer paid for by taxpayers should result in his discharge.

This case illustrates the competing values and interests that this topic invokes. It is too early in our local jurisprudential history to draw any definitive patterns. Simply put, not enough has been adjudicated to date. Employers are just starting to formulate and promulgate Internet Technology (IT) usage policies and unions are just beginning to come to terms with how to react. The few cases that have come to arbitration are applying time-honored doctrines such as judging Internet usage rules against standards of reasonability, equality of enforcement, and compliance with the collective agreement. Further, discipline resulting from Internet use/abuse is being judged against established doctrines such as misuse of company equipment, creating a poisoned work environment, negatively affecting the employer's reputation and whether or not clear rules are in place.

This arbitral approach brings to mind questions: Should the Internet be treated any differently than other workplace issues? How is the Internet any different from an office bulletin board, conversations around the water cooler, telephone conversations, or an employee's letter to the editor of a local newspaper? What makes the Internet different? In many workplaces, employees are allowed some private use of the e-mail system in the same way that they are allowed to use the telephone for some limited personal purposes so long as there is no negative impact on productivity or other employees. Why then is it generally accepted that an employer may be able to monitor employees' e-mails as part of its right to control its resources, yet there would be a visceral reaction against the discovery that an employer was monitoring all telephone calls?

Part of the answer may be that Internet usage is a huge issue. A recent Angus Reid poll reports that 34% of office workers have access

to the Internet and that they spent an average of two hours per week on their employers' equipment for their own personal use.[2] This can peak at times of intense public interest. NetPartners estimated that businesses lost $50 million in worker productivity when the Starr Report and former President Clinton's video deposition were released on the Web.[3] This vast amount of personal use has enormous implications on productivity, effects the security and capacity of a business's network, and risks exposure to viruses. This also makes companies vulnerable to potential liability for illegal activities such as transmission of child pornography, fraud, libel, and Human Rights violations. As a consequence, employers are utilizing technology to conduct systemic monitoring and blocking certain pathways. In order to understand and anticipate how arbitrators will respond to cases involving Internet use in the workplace, it is important to look first at the general principles of privacy and free speech in the Canadian workplace.

## I. WHAT IS THE NATURE AND EXTENT OF FREE SPEECH IN THE ORGANIZED CANADIAN WORKPLACE?

The leading case is *Fraser*.[4] He was employed as a supervisor by Revenue Canada.[5] He publicly criticized the federal government's policies regarding metrification and the entrenchment of the Charter of Rights in the constitution. His refusal to refrain from the criticisms after warnings and two suspensions led to his discharge. The Supreme Court of Canada upheld the discharge, giving us the following principles:

> First, our democratic system is deeply rooted in, and thrives on, free and robust public discussion of public issues. As a general rule, all members of society should be permitted, indeed encouraged, to participate in that discussion.
>
> Secondly, account must be taken of the growth in recent decades of the public sector—federal, provincial, municipal—as an employer. A blanket prohibition against all public discussion of all public issues by all public servants would, quite simply, deny fundamental democratic rights to far too many people.
>
> Thirdly, common sense comes into play here. An absolute rule prohibiting all public participation and discussion by all public

2. *Governments Move to Limit Employee's Internet Access and E-mail Use*, 24 LANCASTER'S COLLECTIVE AGREEMENT REP. No. 1112, Nov.-Dec. 2000, at 1.
3. Dichter & Burkhardt, *supra* note 1.
4. Fraser and Public Staff Relations Board, [1985] 2 S.C.R. 455.
5. The Federal Government's customs and excise agency.

> servants would prohibit activities which no sensible person in a democratic society would want to prohibit.
>
> On the other side, however, it is equally obvious that free speech or expression is not an absolute, unqualified value. Other values must be weighed with it. Sometimes these other values supplement, and build on, the value of speech. But in other situations there is a collision. When that happens the value of speech may be cut back if the competing value is a powerful one. Thus, for example, we have laws dealing with libel and slander, sedition and blasphemy.
>
> . . . . . .
>
> As a general rule, federal public servants should be loyal to their employer, the Government of Canada. The loyalty owed is to the Government of Canada, not the political party in power at any one time. A public servant need not vote for the governing party. Nor need he or she publicly espouse its policies. And indeed, in some circumstances a public servant may actively and publicly express opposition to the policies of a government. This would be appropriate if, for example, the Government were engaged in illegal acts, or if its policies jeopardized the life, health or safety of the public servant or others, or if the public servant's criticism had no impact on his or her ability to perform effectively the duties of a public servant or on the public perception of that ability. But, having stated these qualifications (and there may be others), it is my view that a public servant must not engage, as the appellant did in the present case, in sustained and highly visible attacks on major Government policies. In conducting himself in this way the appellant, in my view, displayed a lack of loyalty to the Government that was inconsistent with his duties as an employee of the Government.

This case was applied recently in the hearing concerning Mr. Chopra and Health Canada.[6] Mr. Chopra appeared at a public conference on Employment Equity and was harshly critical of his employer regarding its treatment of visible minorities. He went so far as to say that anything the Director of Human Resources said "would be a lie." The tribunal considered the nature of the issues raised in Mr. Chopra's remarks and the fact that he was free to file his complaints of racism and discrimination with the Canadian Human Rights Commission. It concluded,

> . . . it is healthy for the Department, for employees within the Department, for the Public Service and for Canadian Society as a whole, that all persons be free to express their differing views to engage in public debate on these matters.

6. Canada (Treasury Board—Health Canada) v. Chopra, 96 L.A.C. (4th) 367 (Public Service Staff Relations Board).

> By clomping [sic] down on individuals who voice their opinions on fundamental issues such as the ones at issue in the instant case (racism; discrimination; employment equity), a department simply risks reinforcing the perception that there is a validity to the claim that racism does exist within that department.

The use of e-mail or the Internet to voice one's opinion against an employer will probably not be a significant factor in deciding upon the propriety of the comments. The content will probably be more important than the context. The discharge of an employee with 15 years' seniority was upheld after he sent e-mails to his employer's parent company's Board of Directors. The e-mails were prompted by the grievor's belief that management had failed to properly deal with his daughter's complaints about discrimination and harassment in the same workplace. After considering the contents of the correspondence, the arbitrator concluded that it was "inflammatory, disrespectful and false in many aspects." The tone of the e-mails was considered to be sufficient to warrant the five-day suspension and subsequent discharge after he failed to discontinue his correspondence. The arbitrator held that it was entirely foreseeable that the grievor's actions would cause embarrassment to his managers and that his genuine belief in the validity of the cause did not justify either the tone or the content of the e-mails.[7] In this case, the medium of the Internet may have facilitated access to the Board of Directors, but the content of the message was the determining factor in the adjudication of the discipline.

In another case, the use of a union "chat line" supplied through the employer's computer system resulted in a discharge. The grievor had used this chat line to viciously attack his employer. The arbitrator found that there would be no reasonable expectation of privacy in this situation because of the medium itself and the fact that messages can be copied.[8] It seems that the use of the Internet was seen to be akin to an employee standing up in the middle of a shop floor and speaking out against the company. The arbitrator treated this as if it were a classic case of insubordination, despite the forum of a union chat line.

Canadian arbitral caselaw has not yet fully addressed the question of whether private e-mails lose their cloak of privacy simply because they are transmitted on an employer's Internet or intranet system. A union counsel argues the case for the employees:

---

7. Communication, Energy and Paperworkers' Union, Local 777 v. Celanese Canada Inc., [Feb. 26, 2001] (Unreported decision of David Jones).

8. Camson College v. Canadian Union of Public Employees, Local 2081, [1999] B.C.C.A.A. 490.

> The proposition that ownership confers the right to oversee every use of equipment is unpersuasive. Use of the employer's phone to make a doctor's appointment does not, for example, entitle management to tape the call or use the medical information for its own purposes. Use of a company pen does not entail a right to read private love letters which happen to have been written with that pen. Nor does use of a washroom situated on company premises afford a right to place surveillance cameras in lavatory stalls to ensure that only approved business is being conducted. The fact that the employer owns the e-mail system does not invariably lead to the conclusion that e-mail which is clearly personal in nature is open to inspection by management.[9]

However, ownership of equipment is factoring into arbitrators' decisions. One arbitrator held that an employee has no "absolute right to privacy" if he or she is using the employer's computer. The decision declared that an employer is entitled to access and examine personal and work-related files on the hard drive of the computer used by the grievor. This monitoring led to the grievor being suspended for engaging in personal activities on company time. The discipline was upheld.[10]

## II. THE STATUTORY FRAMEWORK OF THE "RIGHT" TO PRIVACY AND THE ABILITY TO INTERCEPT "PRIVATE" COMMUNICATIONS

The Canadian *Charter of Rights and Freedoms*[11] provides:

> 2. Everyone has the following fundamental freedoms: . . .
>
> (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; . . .
>
> 8. Everyone has the right to be secure against unreasonable search or seizure.

Canada is a federation where both the federal and provincial governing bodies legislate rights and responsibilities. The statutory right to privacy for people or employees does not exist in all provinces of Canada. For example, the largest and most populous province of Ontario has no statutory right to privacy. However, the federal government has jurisdiction across the country over interprovincial and federal undertakings, including criminal law. Section 184 of the Criminal Code[12] makes it an indictable offense to "willfully intercept a private communication" by means of an electro-magnetic, acoustic, or

9. Lorne Richmond, *Employee Use of E-Mail and the Internet: A Union Perspective*, *in* 2 LABOUR ARBITRATION YEARBOOK 45 (2001-2002).

10. B.S.O.I.W. Local 97 v. Office and Technical Employees [Nov. 12] (Unreported).

11. Constitution Act, SI/84-102 (1982).

12. R.S.C., ch. C-46 (1985) (Can.).

other device. The courts have not yet addressed whether a communication through company-owned equipment would be considered a "private communication." This may depend upon the intent of the sender, the nature of the Internet policies in the workplace, and the expectations of privacy.

As of January 1, 2001, the *Personal Information and Electronic Documents Act*[13] came into force. It applies only to federally regulated industries and the organizations that send personal information across provincial and other boarders. It creates protections regarding the collection, use, or disclosure of personal information in the course of commercial activity. It applies to all federally regulated organizations that collect, use, or disclose personal information in the course of their commercial activities. It has been suggested that this legislation can serve as a guideline in terms of determining what would be appropriate standards to apply to employers' monitoring of employees' Internet use. This Act requires that any monitoring should have the following:[14]

1. Identification and disclosure of the purposes for which personal information is collected.
2. The consent of the individual for the collection of personal information.
3. Limits on the collection of personal information to that which is necessary for the purposes identified.
4. Availability to individuals of company policies and practices regarding the management of personal information.

Employers are developing rules and policies for usage. The nature and extent of these policies will vary depending on the nature of the enterprise, whether the operation is subject to federal or provincial labor legislation and whether it is part of the private or public sector. The differences in these jurisdictions are too complex and broad to deal with in this paper. Suffice to say that for monitoring policies to be considered reasonable and enforceable, they will have to balance the individual's expectations and/or rights of privacy with the employer's right to protect sensitive information and assets (including computers and their networks). In addition, scrutiny will have to be given to ensure that the monitoring conforms with the law. Common sense and established labor relations principles would suggest that

13. Ch. 5, 2000 S.C. (Can.).

14. James G. Knight, Abuse of the Internet and E-mail, Unreported Address to the University of Guelph—Supervisory Program (June 2001) (on file with Mr. Knight).

monitoring policies should be defined and communicated before the practices are implemented. But common sense also would suggest that any reasonable employee would recognize that certain types of Internet usage are well beyond the scope of something the employer would condone in the workplace. Just as arbitrators do not require an employer to post rules against theft before upholding discipline on that ground, one would not expect arbitrators to demand clear rules against using an office Internet system for transmitting hate literature before upholding discipline for such conduct.

A recent case dealing with interception of phone calls may signal how e-mails could be treated. The Hindu Mission was concerned about theft and unauthorized long-distance calls on its premises. As a result, the Mission's executive committee decided to tap the phone lines. This recorded a series of very personal telephone calls between the Mission's married priest and one of its married volunteers. Under the resulting pressure, the priest resigned. Then he and the volunteer sued for defamation and invasion of their privacy rights under the province of Quebec's *Charter of Human Rights and Freedoms*. Section 5 of the Quebec *Charter* provides: "Every person has a right to respect for his private life." The Quebec Court of Appeal applied the provincial *Charter* and the same reasoning that has been applied to the Canadian *Charter's* section 8 protections. It began its analysis by asking if the persons involved had a reasonable expectation of privacy in the conversation. The court held that because the players in this case were confidants and their conversations were not related to professional matters, they had a reasonable expectation of privacy. They were each awarded monetary damages for the violation of their privacy rights.[15] It is clear that the case would have had a different result if the intercepted conversation had revealed discussions related to and/or detrimental to the defendant employer's business.

The concept of the "reasonable expectation of privacy" is fundamental to the Canadian approach to electronic surveillance. It is a major consideration for arbitrators looking at issues of video surveillance.[16] However, a recent case in Ontario has put the parties on notice that at least one arbitrator will not assume or apply the

15. Srivastava v. Hindu Mission of Canada, *as reported in*, Jeffrey Miller, *Off the Record: Workplace Phone Call Protected by Privacy Law?*, THE LAWYERS WEEKLY, July 6, 2001, at 5.

16. Toronto Transit Commission v. A.T.U. Local 113, 88 L.A.C. (4th) 109 (1998) (Shime); *see also* T. Jollife, G. Mecerin, & J. Carpenter, *Privacy and Surveillance: Balancing the Interests; An Arbitrator's Perspective, A Management Perspective and a Union Perspective*, *in* 2 LABOUR ARBITRATION YEARBOOK (1999-2000).

concept of the "right of privacy."[17] One arbitrator analyzed many cases involving the invitation to arbitrators to "balance" the employee's right to privacy with the employer's right to manage and control the workplace. The decision bluntly points out that there is a fundamental difference in common law between a "liberty" and a "right." It concludes that there is no right to privacy unless the statutory protection is legislated:

> I concede that many, indeed most, people in our society have some *expectation* of privacy. However, the common law has never protected privacy as such. Individuals may be at liberty to enjoy privacy, as they are at liberty to speak out against conventional mores, but absent an applicable statute on point, both liberties are likely to be interfered with or suppressed by state sanction or other individuals. The common law focus has been on the method of interference, not on the interference itself. For example, shouting to render someone else's free speech inaudible is not actionable; physical suppression is. . . .
>
> The issue in this case is the admissibility of videotape evidence that may show the Grievor, outside the workplace, engaging in various physical activities inconsistent with his claimed disability. The making of the videotape may well have violated the Grievor's expectation of privacy, and probably interfered with his liberty of privacy. However, under the common law of Ontario, the Grievor had no right of *privacy*. Consequently, any claim that the evidence is inadmissible because it was obtained in violation of a right of privacy must fail. The arbitration cases that say otherwise are, in my view, wrong. (p. 149)

Other approaches that have been applied to the challenge of camera placements in a workplace may be relevant to Internet monitoring. In a decision where the arbitrator found that there was no "free-standing right of privacy to justify the union's request to remove . . . internal cameras," he also concluded that the union's challenge to the placement of the cameras was arbitrable and subject to review on three grounds:

1. The management rights clause of the collective agreement gave the employer the right to make "reasonable rules." Under that provision, the union can challenge the reasonableness of a rule that employees must subject themselves to camera surveillance if they wish to work.
2. It is appropriate for a union to bring forward a policy grievance alleging that the employer has not fulfilled the

17. *See* Canadian Timkin, Ltd. v. United Steelworkers of America, 98 L.A.C. (4th) 129 (2001) (B. Welling).

general requirement of exercising its management rights in a reasonable manner.

3. The employer's action is subject to challenge for not being based on a legitimate business interest.[18]

When dealing later with the merits of the issue, the arbitrator concluded that the placement of the cameras was unreasonable:

> . . . there is a pervasive repugnance to the use of electronic surveillance of employee work performance. I think it is proper to take, as it were, quasi-judicial notice of the fact for the last 20 years, employers have generally found that their own interests, in terms of both productivity and employee morale, are best served by adopting less rigid, mechanistic, authoritarian hierarchical and impersonal approaches to the organization of work and the management of their enterprises. Surreptitious surveillance, by electronic means, runs counter to this trend.

The jurisdiction to review the placement of surveillance cameras has also been founded under a collective agreement provision that promised the maintenance of "operational practices" unless there was mutual agreement to the changes.[19] Both the Ontario Labour Relations Board and an interest arbitrator have also expressed serious concern about the placement of the "electronic eye" into the workplace.[20]

Unions have long taken the position that camera surveillance is a "despised device for monitoring the workforce."[21] One has to wonder, however, whether there will be a change in this perspective. Video cameras are now accepted methods of ensuring safety. Some organizations that once challenged the installation of video cameras now welcome them as assisting in the maintenance of safety. Cameras now exist in banks, shopping centers, food stores, transportation terminals, schools, and colleges as a matter of course. Earlier objections to their placement have been withdrawn. If concepts like the reasonable expectations of privacy, legitimate business purposes, and reasonable exercise of management rights are being applied, they will be applied in the context of the particular workplace and the climate of the day. With the increased risks of violence and safety concerns, there may be a softening of attitudes towards surveillance in general.

18. Lenworth Metal Products, Ltd. v. U.S.W.A., Loc. 3950, 80 L.A.C. (4th) (1999) (T.E. Armstrong).

19. Thibodeau-Finch Express, Inc. v. Teamsters Union, Local 880, 32 L.A.C. 271 (1988) (Burkett).

20. Purtex Knitting Co. v. Canadian Textile and Chemical Union, 23 L.A.C. (2d) 14 (1979).

21. Richmond, *supra* note 9.

## III. ARE PERSONAL COMPUTER FILES AND E-MAILS COMPELLABLE AS EVIDENCE?

Sections 48(12)(b) and (f) of the Ontario *Labour Relations Act* give an arbitrator the power to order production of any "documents or things" that may be relevant to the matter and accept evidence that the arbitrator considers proper, "whether admissible in a court of law or not." It is also interesting to note Criminal Code Section 278.5(2) that deals with ordering production of records including personal journals and diaries in the context of sexual offence trials. It instructs the judge to:

> . . . consider the salutary and deleterious effects of the determination on the accused's right to make full answer and defence and on the right to privacy and quality of the complainant or witness. . . . In particular, the judge should take the following factors into account:
>
> (a) the extent to which the record is necessary for the accused to make a full answer and defence;
>
> (b) the probative value of the record;
>
> (c) the nature and extent of the reasonable expectation of privacy with respect to the record
>
> (d) whether production of the record is based on a discriminatory belief or bias;
>
> (e) the potential prejudice to the personal dignity and right to privacy of any person to whom the record related;
>
> (f) society's interest in encouraging the reporting of sexual offences;
>
> (g) society's interest in encouraging the obtaining of treatment by complainants of sexual offences; and
>
> (h) the effect of the determination on the integrity of the trial process.

Arbitrator Michel Picher reviewed this statutory framework in a recent preliminary award[22] that dealt with the issue of whether the employer could seek production of the grievor's personal diary of events in the workplace. The grievor's habitual making of the diary entries during critical events had been one of the grounds for her discharge. Mr. Picher acknowledged that a board of arbitration is not a criminal court, but he concluded that arbitrators should consider the Criminal Code as an "instructive and useful" guide in the exercise of discretion regarding the admission of evidence. In addition, he

22. Ontario Power Generation v. Power Workers' Union, 97 L.A.C. (4th) 90.

applied the Supreme Court of Canada's[23] guidelines for the admission of confidential documents. They can be summarized as follows:

1) The party seeking production must satisfy the test that the material sought is "likely to be relevant" to the issue at hand

2) To be considered confidential, the communication must
   - originate in a confidence
   - the confidence must be essential to the relationship in which the communication arises
   - the relationship must be one which should be "sedulously fostered" in the public good

3) If the relevancy test is met, the adjudicator makes a private scrutiny of the documents to determine which portions should be admitted
   - by balancing the "constitutional right to privacy" in the information on the one hand, and the right to a full answer and defence on the other, and
   - by considering whether the interests served by protecting the communications from disclosure outweigh the interest in getting at the truth and disposing correctly of the litigation.

4) The interest in disclosure of a defendant in a civil suit may be less compelling than the parallel interest of an accused charged with a crime. Therefore, the balance between the interest in disclosure and the complainant's interest in privacy may be struck at a different level in the civil and the criminal case.

In the context of the dismissal arbitration, Arbitrator Picher concluded that personal notes and diaries should be accorded the status of confidential documents. Further, a board of arbitration should only direct production under the conditions and safeguards reflected in these cases and Criminal Code as set out above. He added that arbitrators should also consider:

- The extent to which the evidence would be necessary to the Company's discharge of its burden of proof.
- The probative value of the evidence.

23. R. v. O'Conner, [1995] 4 S.C.R. 411; M. (A) v. Ryan, [1977] 1 S.C.R. 157.

- The extent to which the documents in question were formulated with a reasonable expectation of privacy.
- The potential prejudice to the dignity and right of privacy of the grievor by the release of the material.
- Keeping in mind that the board of arbitration is the master of its own procedure, the extent to which an order for or against production might impact on the integrity of the arbitration process.

One could expect that arbitrators would treat the personal notes or journals that an employee may keep in a personal file on their office computer in the same way.

## IV. ARBITRAL TREATMENT OF INTERNET USE/ABUSE BY EMPLOYEES

Overuse of the Internet is being accepted as an employment offense. Whether or not policies are in place dictating the amount of permissible time, excessive time spent on non-work related Internet explorations is treated as grounds for discipline. Discharges are being upheld where there is accessing of pornographic sites and/or dishonesty in the course of the investigation.[24] Lesser consequences such as a one-day suspension are also being accepted.[25] In a case where the employer argued that the essential employer/employee trust had been broken by the grievor's excessive Internet use, the arbitrator found that reinstatement was viable and appropriate because the employer could monitor the grievor's Internet use after reinstatement.[26] None of these cases question the employer's ability or right to monitor for misuse. Indeed, the last case relies on the ability to monitor as the basis for assuming that repeats of the misconduct will not occur.

Arbitrators are treating the invasion of privacy via the Internet more seriously than the abuse of the Internet itself. An employee of Canadian Pacific Railway used the Internet to send sexually intimate messages to another employee who was his girlfriend as well as to transmit derogatory gossip about coworker. In addition, the same employee was party to an unauthorized access of yet another

24. Calgary Regional Health Authority v. Health Science Ass'n of Alberta, [1999] A.G.A.A. No. 66; Dupont Canada, Inc. v. C.E.P., Local 28, 92 L.A.C. (4th) 261 (2001) (E. Palmer).

25. British Columbia Gov't v. B.C. Gov't Services Employees Union, [1998] B.C.C.A.A.A. 535 (Maddison Grievance).

26. Chronicle Journal v. Thunder Bay Typographical Union, Local 44, [2000] O.L.A.A. 575.

employee's computer files.[27] The employer failed to prove that it had communicated a clear policy or system of rules regarding the use of e-mail for personal messages. This was considered as a mitigating factor. The arbitrator held that given that the messages to the girlfriend were intended to be confidential, a "relatively light measure of discipline" would be appropriate even though they amounted to distasteful "electronic graffiti." However, the arbitrator concluded that more severe discipline was warranted for the violation of another employee's computer files. The girlfriend was also disciplined for engaging in electronic "chit-chat" that could be offensive to other employees. Her discipline was reduced to a written warning. The basis for her discipline was the risk of potential offense to other employees:

> There is clearly a different order of risk and harm to others when negative or insulting comments are placed upon an electronic e-mail system which, notwithstanding its security, can be accessed by others, than, for example, engaging in idle gossip in a private one-on-one conversation.[28]

In a third Canadian Pacific Railway case,[29] a significant penalty was upheld against an employee for using the e-mail system to obtain answers to a correspondence apprentice course he was taking in conjunction with the employer to further his career. He also corresponded with his friends even though he was not authorized to use e-mail for that purpose. The employer considered the nature and the contents of this latter correspondence to be offensive and inappropriate. This correspondence was described by the arbitrator as "not altogether unusual for a 26 year old" and reflecting a "mild case of barracks' humour." The employer had combined the two series of incidents and discharged the employee. The arbitrator agreed that serious discipline was warranted for the improper use of the Internet to obtain test answers. However, the arbitrator concluded that the "offensive" correspondence was insufficient reason to elevate the discipline to a discharge. The arbitrator also refused to agree with the employer that this amounted to "theft" of equipment or resources.

However, opening someone else's e-mail, even in a system where everyone had been given a default password, was considered to be

27. Canadian Pacific Ltd. v. Transportation Communications Union, Canadian Railway Office of Arbitration, Case No. 2732, (1996) (M.G. Picher, Arb.).

28. *Id.*

29. Canadian Pacific Railway Company v. Int'l Brotherhood of Electronic Workers, Canadian Railway Office of Arbitration, Case No. AH-473 (2000) (M.G. Picher, Arb.).

sufficient grounds for discharge. This was held to be akin to opening personal mail on someone's desk and/or impersonation of the proper user.[30]

The use of e-mail as a means of sexual harassment is both a predictable result of the technology and yet another employment problem. A man with 24 years' seniority used the company's internal e-mail system to send anonymous sexually explicit messages to a female employee. At times he also used another employee's initials to suggest someone else was the author. The company's IT department had little trouble tracing the culprit. His conduct was considered to amount to sexual harassment. But the discharge was reduced to a significant suspension with no compensation on the basis of his seniority and the fact that the shame of his exposure had had such a devastating effect on his reputation in the workplace. The arbitrator called this a "borderline case"[31] where the decision could have easily gone against the grievor because of the seriousness of the misconduct.

The improper use of e-mail has also been held to be a breach of trust. An employee who accessed her supervisor's e-mail on several occasions to learn why she had not been promoted was considered to have committed a breach of trust. The arbitrator upheld the dismissal of the grounds that the action had destroyed the viability of a continued employment relationship despite 20 years of seniority.[32]

These cases show a respect for the privacy of computer files and that invasion of that privacy will be treated as a serious employment offense. However, the cases also operate on the assumption that there is really no privacy in the e-mail system and that users should recognize that what may be intended as private correspondence might well be treated as if they were notes posted on an bulletin board in the company's lobby. One arbitrator has held that, absent clear and established rules, the test for determining what a reasonable employee would understand to be an appropriate use of e-mail would be whether the receiver or sender would want the message to be made public in the workplace.[33] This suggests that one cannot assume that there is any privacy at all in an e-mail system.

On the other hand, this brings to mind the argument raised in a criminal trial against the admission of video surveillance tapes that

30. Fraser Valley Regional Library v. CUPE, Local 1698 (2000) (unreported decision of E. Burke).

31. Westcoast Energy, Inc. v. CEP, Local 686B, 84 LAC (4th) 185 (1994) (K. Albertini).

32. Fraser Valley Reg'l Library v. CUPE, Local 1698, 91 LAC (4th) 210 (2000) (Burke).

33. Insurance Corp. of British Columbia v. Office and Technical Employees Union, Local 378 (1994) (J. Weiler).

revealed theft of material from a stock room. The same tape also revealed two other employees were using the stock room for sexual exploits. The criminal defense lawyer argued that the fact that others were prepared to carry on an affair in this stock room proved that there was a "reasonable expectation" of privacy in that area. Therefore, he argued that tapes of any activity in the area should not be admissible. Could it also be said that the very fact that employees are willing to carry on intimate or personal communications over Internet systems is indicative of a reasonable expectation of privacy?

## V. ELECTRONIC PORNOGRAPHY

This subject is treated as a category unto itself. Perhaps because of its moral taboo and because of some of its illegality, the cases concerning storage, downloading, and distribution of pornography or sexually explicit material do not even discuss issues of privacy.[34] The cases do not yet challenge the assumption that the employer has the right to monitor and discipline employees for using computer systems for purposes of sexual gratification. Further, the parties and the arbitrators are invoking the traditional concepts of protecting against a poisoned environment and limiting damage to a corporation's reputation.

A woman was discharged after receiving and distributing material that the company characterized as pornographic.[35] Management had become aware of the material after the offending files had tried to pass through the company's computer system and crashed the company's gateway. The arbitrator was prepared to accept the grievor's evidence when she claimed that she had not viewed the material. But the arbitrator concluded that the grievor knew the nature of the material that she passed on to others, both within and outside the company. Further, it was held that the grievor's distribution of the material gave her a responsibility for its contents. The grievor was also held culpable for accepting "objectionable material" from others because of her active participation in a "joke-club." On the other hand, the arbitrator placed blame on the employer for allowing a "permissive atmosphere" regarding personal use of the e-mail system. This was a mitigating factor that led to the reduction of the discharge to a thirty-day suspension. The length of

34. Possession and transmission of child pornography in Canada is illegal. Possession of other forms of sexually explicit material may not be illegal *per se*.

35. Consumers Gas and Communication, Energy v. Paperworkers Union, (Aug. 5, 1999) (unreported decision of Belinda Kirkwood).

the suspension appears to have been based on the seriousness of distributing the material outside the company and the potential harm that this could cause to the company's reputation.

Lest there be any doubt, possession and distribution of child pornography is a criminal offense. When a computer transmits child pornography, it is considered as a "visual representation" within the meaning of the Canadian Criminal Code. Proof of possession will result in a criminal conviction.[36] Proof of possession involves the concepts of knowledge and control. Employers and employees alike are susceptible to conviction if it can be proven that such files are known to be within their control.

Questions arise about whether the materials are properly considered pornographic. In one case, an employer had a policy against employees downloading "sexually explicit and pornographic material."[37] However, the arbitrator considered the photographs in question to be more akin to the pictures of scantily clad young women that often appear as regular features of some Canadian newspapers' third pages. While the grievor's conduct was found to offend the employer's computer usage policy, the nature of the material was not considered to be pornographic. The grievor had been disciplined on a previous occasion for breach of the same policy. His discharge for these pictures was reduced to a four-month suspension to reflect the seriousness of the offense, to satisfy the aim of deterrence and to correct the employer's overreaction to the material.

Some argue that the consensual nature of the exchange of sexually explicit material removes the conduct from the realm of misconduct. Employees often trade jokes and photographs that strain the lines of definition of propriety. Arbitrators are concerned about the impact on the workplace. This was explained in a recent decision:

> The nature of the material is an important consideration. While some might argue "beauty is in the eye of the beholder" (or at least the pornographic equivalent of beauty), this is only part of the issue. That is because the employee disseminating such material maintains little control over who the beholder might be. An Employer has a legitimate interest in preventing its employees from exposure to materials of this type. This exposure might occur as a result of it being sent to a co-worker who, contrary to the sender's expectations, found it offensive. This might occur accidentally or indirectly, as it did here where managers discovered it or had to deal with it as part of their legitimate activities. This

36. R. Weir, Alberta Court of Queen's Bench, [1998] 213 A.R. 285.

37. Dupont Canada and Communication, Energy v. Paperworkers Union, Local 28-0, [2001] O.L.A.A. 676 (No A/Y 10059).

> also might occur by accident, as it is not uncommon for e-mail messages to accidentally get sent to the wrong recipient or even a list of recipients.
>
> Many view experience of this type of material as a form of workplace harassment particularly because of the degrading manner in which it portrays women. The Employer is subject to a legal duty to prevent such harassment, including that which arises by unintended but avoidable exposure. . . .
>
> The grievor also relies on the proposition that no one complained and no one was hurt by his having sent out these materials. This is basically a "we were all consenting adults" defence. I accept as true that none of the direct recipients complained. . . . The employee is perfectly free to circulate such material with other consenting adults away from work, but I do not find that line of defence persuasive in the workplace, on company time and equipment and particularly in the face of an express warning.[38]

A fascinating development in this area is the defenses that are being raised when employees are found to be downloading pornographic files. Unions are arguing that obsessive use of the Internet is a "disease" or an addiction requiring accommodation by the employer. The duty to accommodate and the definition of what constitutes a disability have been given a very broad and liberal interpretation in Canada. Employers are required to accommodate disabilities up to the point of "undue hardship." In a recent case,[39] an employee was discharged for accessing pornographic sites and spending "unacceptable amounts of time" on inappropriate activities on the employer's Internet server. His union raised the following defenses:

- that he has a "handicap" within the meaning of the Ontario *Human Rights Code,*
- that his viewing of pornography on the Internet at work was causally related to that handicap, and
- that therefore his termination [of employment] for viewing pornography, without any accommodation of his handicap or even any consideration of it, was in violation of the *Human Rights Code* and the anti-discrimination provisions of the collective agreement.

On the basis of unchallenged medical evidence, the arbitrator concluded that the grievor suffered from:

38. Telus Mobility v. T.W.U., 102 L.A.C. (4th) 239 (2002) (Sims).

39. Corp. of the City of London v. CUPE, Local 101 (Oct. 2001) (unreported decision of William A. Marcotte).

> . . . an underlying psychotic disorder that has been diagnosed as 'paranoid schizophrenia' or which 'appears as a schizophrenia-like illness . . . as well [as] longstanding anxiety disorder symptoms of obsessionality and compulsive traits that fulfill obsessive compulsive disorder criteria, according to internationally-accepted standards for diagnosis of psychotic disorders. . . .'

The linkage of the grievor's condition to his behavior caused the arbitrator to conclude:

> I find that there exists a causal link between the grievor's mental condition and the behaviour, viewing pornography on the Internet during working hours, that attracted discipline from the Employer. I find that the grievor's obsessive/compulsive symptomatology associated with his psychotic disorder impaired the grievor's rationality. In that regard, I note Dr. Cortese's evidence that individuals with the grievor's compulsivity/obsessionality disorder "not may, but do know [their actions] are irrational." I find that the grievor's rationality was impaired by his mental condition and that his behaviour which attracted Employer discipline is causally linked to his mental condition. I therefore find that the grievor's mental condition is properly a mitigating factor in the instant case.

The grievor had ten years of seniority and there was evidence of a favorable medical prognosis. The arbitrator substituted a five-day suspension for the discharge. The reinstatement was conditional upon the union presenting medical evidence to the employer indicating that the grievor was successfully continuing upon the course of prescribed drug therapies that could control his inappropriate actions. This case clearly turned on the unchallenged expert medical evidence called by the union. While the result may appear surprising at first blush, it is simply the application of the traditional concept of using a medical condition as a mitigating factor. It will be interesting to see where else this medical approach may take us. Other arbitrators have not been persuaded that "Internet addiction" is a disease.[40]

Another aspect to note in this area is the employer's ability to acquire the evidence against employees. There seems to have been little challenge of the employer's ability to monitor computer usage and to file the material as evidence. But one area to watch may be challenges to the evidence. There is no reason to ignore the traditional requirements of proof. The fact that the material may be offered as being connected to a certain employee or that it is alleged to contain certain data may still be open to challenge.

40. G.T.A.A. v. P.S.A.C., 101 L.A.C. (4th) 124 (2001) (Murray); Seneca College v. OPSEU, O.L.A.A. 415.

Further, the ability to monitor in itself has been held to put an onus on an employer to gather all available evidence against an employee before taking disciplinary action or risk the ability to call further acquired evidence. In the *Dupont Canada*[41] case, the interesting results of the employer's search of the grievor's computer files after he was discharged for violations of the employer's computer usage policy were ruled inadmissible. The arbitrator applied the traditional concept that after acquired evidence is only admissible if it could not have been known or discovered before the discipline was imposed. In this situation, the arbitrator considered the fact that the ability to monitor the employees' computer files was available to this employer before it decided to discharge the grievor. Simply put, the evidence being tendered could have been uncovered earlier. Therefore, the employer was precluded from bolstering its case with material acquired after the discharge.

## VI. FURTHER IMPLICATIONS OF THE ABILITY TO MONITOR

The technology that creates Internet systems also allows those systems to be monitored. The implications of this ability to monitor affect more than the immediate workplace. A fascinating dispute is evolving in Ontario concerning the implications of the information technology policies and practices of the Crown in Right of Ontario (the "Crown"), the employer of the provincial civil service, and The Association of Management, Administrative and Professional Crown Employees of Ontario (AMAPCEO). The Crown's IT policy reads that "access is intended for government business and ministry or agency approval is required." Under this auspice, the Crown has allegedly prohibited and blocked electronic mail communication between AMAPCEO and its members over Crown computer equipment. The Association filed a complaint before the Ontario Labour Relations Board (OLRB) alleging that this amounts to an unfair labor practice by unlawfully interfering in the Association's representation of its members. Before the matter could be heard on its merits, the Association brought a preliminary motion asserting that the OLRB could not fairly adjudicate the matter because the Board itself has an interest in the outcome of the case because all of the OLRB adjudicators are subject to the same IT policies.[42] Further, it

41. *Supra* note 23.

42. Crown in Right of Ontario (as represented by Management Board of Cabinet and Association of Management, Administrative and Professional Crown Employees), OLRB File 1581-00-U, (Oct. 1, 2001) (M.E. Cummings, Alternate Chair).

was asserted that the IT policies give the Crown the technical ability and the right to monitor and gain access to the private notes, e-mail, and draft decision of the OLRB members. Therefore, it was asserted that the Board does not have the institutional independence from the Crown to be able to hear and determine a matter in which the Crown is a party. The Crown's position was that although it may have the technical ability to access or monitor adjudicators' notes and draft decisions, this would be contrary to its IT Policies.

The OLRB's decision reviewed the jurisprudence that recognizes the importance of protecting the privacy and sanctity of the adjudicative decision making process. However, the Board concluded that none of its adjudicators shared an interest in the result or the remedies being sought by AMAPCEO. While the Board acknowledged that prohibiting the Crown from monitoring the Board's computers would advantage its adjudicators, the Board drew a distinction between "being affected by an outcome" and "having an interest in it." The Board went on to conclude that:

> In order to achieve an appropriate degree of institutional independence, the Board need not control all aspects of its administration, only those that are directly related to adjudication. Security of notes and draft decisions are administrative matters that directly relate to adjudication. But I do not think it follows that the Board has to have its own computer network in order to control the security of adjudicators' work in progress. It is enough if the Board ensures that the provider of the network has policies and mechanisms in place that prevent outsiders from accessing adjudicators' work, and the Board makes sure that the policies are followed.
>
> I am satisfied that the Crown's IT policy, as it is exercised with respect to the Board . . . . does not constitute an inappropriate challenge to the Board's independence. The Crown has the technical ability to read computerised text files, but it is contrary to its IT policy to scrutinise such files in the course of carrying out general network monitoring. No doubt, someone outside of the Board has a key to the office in which I work, and is capable of opening the door, and looking at any work in progress stored there. But it would be wrong for someone to do so. In my view, that situation is not fundamentally different from the facts put before me.

The impact of this decision is hard to predict. The decision has engendered a great deal of controversy. The litigation should itself be recognized as arising in a climate of intense distrust and animosity. However, the case should not be dismissed as relevant only to the political climate of the time. One should not underestimate the importance of the fact that adjudicators are being asked to rule upon

not only the validity of IT usage policies, but also the implications of their potential abuse by those with the ability to monitor and effectively invade the privacy of all users.

The hearing still pending into the merits of this case may be even more interesting and important. It raises issues concerning the use of the Internet by unions for their organizational, business, and administrative purposes. Cases already deal with the ability of unions to carry on business on company premises, utilize company bulletin boards, and use company equipment. The traditional approach of labor relation's tribunals has been to hold that a blanket prohibition against union solicitation by individuals upon the employers' premises constitutes unlawful interference with employees' right to organize.[43] Employees are allowed to use their own time to solicit coworkers so long as this does not interfere with the employers' business interests.[44] The Canada Labour Relations Board upheld the right of union supporters to distribute material through the company's internal mail system because the employer had previously allowed this for both business and personal communications.[45] Would the same principles apply or does the utilization of the company's electronic medium alter the situation? Will arbitrators uphold the right of management to prevent any type of union business from being conducted on the company's network? Would this extend to all forms of union activities, from the simple announcement of a meeting to the organization of strike activities? What would be the response to a union trying an organizational drive through a company's internal e-mail system by sending "personal" messages to all employees? Assuming a best case scenario where the company allowed some reasonable personal use of the e-mail system, would this kind of activity be viewed as private and under the rubric of the "reasonable expectation of privacy?" Or would this type of campaign entitle the employer to monitor and discipline the organizers for misuse of company resources? These are all-important questions that have not yet been addressed in the context of the Internet in Canada.

## VII. IS THE MEDIUM THE MESSAGE? *OR* IS THERE ANY LEGAL DIFFERENCE BETWEEN E-MAIL AND "SNAIL" MAIL?

One judge has suggested that the nature and ease of e-mail as a medium may have implications on the text contained in the message.

43. Comino Ltd. v. C.A.I.M.A.W., [1981] 3 Can. L.R.B. 499 (B.C.L.R.B.).
44. *Id.*; T. Eaton Co. Ltd., [1985] O.L.R.B. 3-491.
45. American Airlines, Inc. v. B.R.A.C., [1981] 3 Can. L.R.B. 3 (C.L.R.B.).

In a civil wrongful dismissal suit, an issue arose about whether the plaintiff had resigned. He had been engaged in an escalating series of insulting e-mails with management about his office space. The critical e-mail stated that he did not "wish to be a part of any organization that not only accepts, but encourages and rewards this type of selfish attitude." His employer treated this as a letter of resignation. The trial judge found that there was no intention to resign. More significantly, he described the e-mail as "emotional and understandable in the circumstances" and that "inappropriate statements are the predictable result of technology which allows instant and unconsidered responses."[46] This decision shows a recognition of the unique media that the Internet provides. E-mail allows for the instantaneous transmission of ideas. That is one of its strengths. But it also discourages the moment of sober second thought that often occurs while one searches for an envelope. This leaves the question as to whether the result would have been the same if the same letter had been sent by post or inter-office memo. Do words really have a different meaning if we have to go to the trouble of finding an envelope and stamp, rather than pushing one "send" button with a mouse? This would have enormous implications on the capacity to contract via the e-mail. Could I rescind an offer by saying that I really did not mean what I said in my last e-mail?

## VIII. IS THERE ANY PRIVACY NOW THAT THERE IS THE INTERNET?

Life is sometimes stranger and more interesting than fiction. A school bus driver working for a company that served the local elementary Roman Catholic School Board engaged the services of an "erotic photographer" to take pictures of her and her husband engaged in sexual acts in various places, including on her school bus. The photos were intended for the couple's private use only. Unknown to them, the photographer put some of their photos on his Web site a few months later. Some local parents came across the pictures, recognized their children's school bus and driver, and then filed complaints with the school board. (No explanation was given as to how or why these parents came to view this site.) As a result of the complaints, the bus driver was fired. The arbitrator accepted her evidence that she had never authorized such use of her photos. But there was a finding that the existence of these pictures and the

46. O'Neil v. Towers Perrin, Ontario Superior Court, 2119-010, 108 A.C.W.S. (3d) 98 (2001).

community's knowledge of this "could undermine her authority as a school bus driver." Her discharge was upheld.[47]

What does this case tell us? Perhaps the lesson is that the advent of the Internet has meant the erasure of any semblance of privacy. Further, any actions that are capable of being captured in a form that can be transmitted via technology expose us (no pun intended) to the consequences of that public forum.

## IX. WHAT PRIVACY IS LEFT TO THE EMPLOYEE?

Canada's former Privacy Commissioner spoke about "privacy" in the following terms:

> Privacy . . . is a fundamental human right, recognized as such by the United Nations. But it is not only an individual right—it's also a shared value, a social, public good. In the words of the Supreme Court of Canada, privacy is "at the heart of liberty in a modern public state."
>
> That is because there can be no real freedom without privacy. If at any given moment someone—particularly agents of the state—may be metaphorically or quite literally looking over our shoulder, we are not truly free.[48]

But as the champion of privacy, Commissioner Radwanski also recognized that there is sometimes a need for "privacy-invasive measures" to meet security threats that are concerning us all now. He suggests that any legislative or law enforcement proposals that affect privacy should be weighed against tests of

- necessity
- effectiveness
- proportionality
- severity

These concepts may well have application in the workplace in terms of assessing the reasonability of any monitoring. In terms of the workplace itself, Commissioner Radwanski cautioned:

> . . . if privacy is a fundamental human right and social good, that right does not disappear when we pass through the door of the workplace. I cannot imagine a place where our rights need to be more respected than in the workplace, where we spend so much of our time and where so much of our life is defined. We as a society

47. Bader Bus Service, Ltd. v. Reavely, C.L.A.D. 648 (2000) (B. Etherington).

48. George Radwanski, A New Era of Privacy Protection, Address to the Treasury Management Association of Canada, 19th Annual Finance and Treasury Management Conference (Oct. 2001) *available at* http://www.privcom.gc.ca/speech/02_05_a_011001_e.asp.

> don't tolerate discrimination in the workplace, or harassment. Why would we tolerate invasion of privacy?[49]

But reality must be faced. So far I have addressed the relatively new technology of the Internet and electronic monitoring. But in truth, these concerns are already outdated. We now have wireless technology. Many companies now equip their employees with laptops to allow for greater flexibility and productivity. These laptops can be fitted with an inexpensive "hub" that allows for remote connections to the network. These hubs create "wide-open wireless networks" or a virtual "broadcast station" that are easily susceptible to infiltration.[50] Wherein is the privacy if systems are so vulnerable to penetration? It is ironic that we are discussing how to deal with traditional notions of privacy while the advances that are coming onto to the market put in question the very existence of the concept.

## X. CONCLUSION

Canadians often criticize ourselves for failing to be leaders. Yet Canadian arbitrators are often applauded for being balanced and sensitive to emerging new issues. Canadian arbitrators follow the philosophy of the Canadian chicken that was asked why she was crossing the road. She answered, "To get to the Middle."

The cases decided to date show attempts to balance employer and employee rights on the issues of Internet use in the modern workplace. But many new issues are emerging and we have just seen the tip of the iceberg in terms of what must be sorted out.

The Internet is new, exciting, mysterious to many, and opens new vistas for the workplace and society as a whole. But we should not be too awed by it or forget our traditional and trusted principles of justice and balance. As an American academic recently said:

> We've all heard that a million monkeys banging on a million typewriters will eventually reproduce the entire works of Shakespeare. Now, thanks to the Internet, we know this is not true.[51]

49. George Radwanski, *Workplace Privacy: A New Act, A New Era*, *in* 2 LABOUR ARBITRATION YEARBOOK 1 (2001-2002).

50. Andrew Wahl, *Big Hack Attack: Beware! Your Company's Wireless Network May Leave You Wide Open to Drive-by Hackers*, CANADIAN BUSINESS, Oct. 29, 2001, at 107.

51. Robert Wilensky, *Mail on Sunday*, *in* QUOTES OF THE WEEK (Feb. 16, 1997).