CHAPTER 8

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

PAULA KNOPF*

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

Introduction

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 issue of 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 (IT) 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 our privacy. Further, whereas employers have the right to control the use of their equipment and resources, employ-

*Member, National Academy of Arbitrators, Toronto, Ontario, Canada. This paper was delivered at the Academy's members-only Continuing Education Conference in Tampa, Florida, in November 2001.

ees 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.

Here we will look at the Canadian labour relations community's perspective on these interests. The popular press recently reported a number of interesting cases that bring this topic to mind. For example, a highly ranked and respected member of our military was demoted after revealing that he had used a military issued laptop computer, but his own private Internet account, to access a soft porn site. This came to light when he was called on to discipline a subordinate for misuse of the e-mail system. The public outcry in the press, both for and against this man, 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 porn site on a computer paid for by taxpayers should result in his discharge. His fate has not yet been determined or revealed to the public.

This case illustrates the competing values and interests that this topic invokes. It is too early in our local jurisprudential history to discern any definitive patterns. Simply put, there has not been enough adjudication to date. Employers are just starting to formulate and promulgate 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-honoured 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 and 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 clear rules are in place.

This arbitral approach brings to mind several questions. Should Internet usage be treated differently from other workplace issues? How is the Internet any different from an office bulletin board,

---

[1]Mark S. Dichter & Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, Morgan, Lewis & Bockius (2001), available at <http://www.morganlewis.com>.

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. 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 percent of office workers have access to the Internet and that they spent an average of 2 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 U.S. 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, affects the security and capacity of a 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 Code violations. In response, employers are utilizing technology to conduct systemic monitoring and are blocking certain pathways.

What Is the Nature and Extent of Free Speech in the Organized Canadian Workplace?

The leading case in this area is *Fraser & Public Staff Relations Board*,[4] where a supervisor for Revenue Canada 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:

---

[2]*Governments Move to Limit Employee's Internet Access and E-Mail Use*, 24 LANCASTER'S COLLECTIVE AGREEMENT RPTR. No. 1112, Nov./Dec. 2000, at 1.

[3]Dichter & Burkhardt, *supra* note 1.

[4]*Fraser & Public Staff Relations Bd.*, [1985] 2 S.C.R. 455.

> 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 servants would prohibit activities that 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 Dr. Siv Chopra and Health Canada.[5] Dr. Chopra appeared at a public

---

[5] *Canada (Treasury Board—Health Canada) & Chopra*, [2001] 96 L.A.C.4th 367 (Public Serv. Staff Relations Bd.).

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 would have said to the conference earlier "would be a lie." The tribunal considered the nature of the issues raised in Dr. 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 that

> 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.
>
> 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 to voice one's opinion will probably not be a significant factor in deciding the propriety of comments. The discharge of an employee with 15 years of seniority was upheld after he sent e-mails to his employer's parent company's board of directors that the arbitrator considered "inflammatory, disrespectful and false in many aspects."[6] 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. The tone of the e-mails was considered to be sufficient to warrant the 5-day suspension and subsequent discharge after the grievor failed to discontinue his correspondence. The arbitrator held that it was entirely foreseeable that his 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. In this case, the medium 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,[7] the use of a union chat line supplied through the employer's computer system resulted in a discharge. The

---

[6] *Communication, Energy & Paperworkers' Union Local 777 v. Celanese Canada Inc.* (unreported) (Jones, Feb. 26, 2001).

[7] *Camson College v. Canadian Union of Public Employees Local 2081 (Metcalfe Grievance)*, [1999] B.C.C.A.A. No. 490 (Germaine).

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. It seems that use of the Internet there was seen to be akin to an employee standing up in the middle of a shop floor and speaking out against the company. It is treated as a classic case of insubordination, despite the forum of a union chat line.

Canadian arbitral case law 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 system. A union counsel argues the case for employees:

> The idea that ownership of a tool gives the owner the right to oversee every use of that tool is not convincing. The use of an employer's phone to make a doctor's appointment does not give the employer the right to tape the call and use the medical discussion for its own purposes. The use of a company pen does not give the company the right to see your private letter written with that pen. The use of a company-owned lavatory stall does not give the company the right to install surveillance cameras in the stall to ensure that only company-approved business is being conducted therein. In the absence of reasonable cause to believe conduct worthy of discipline is taking place, the fact the company owns the e-mail system does not immediately suggest that e-mails that are clearly private and personal are open to inspection by the employer. [8]

The Statutory Framework

The Right to Intercept

The Canadian Charter of Rights and Freedoms[9] 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.

---

[8]Lorne Richmond, *Surveillance of Employees, the Workplace and the Computer: Nineteen Eighty-four Comes to the Workplace*, Address to the Canadian Bar Association Ontario Conference on Canadian Corporate Counsel and Labour Relations, June 12, 2001.

[9]S.O. ch.1, sch. A, as amended (1995).

There is no statutory right to privacy for employees in all provinces of Canada—Ontario has no such right. However, section 184 of the Ontario Criminal Code[10] makes it an indictable offence to "willfully intercept a private communication" by means of an electromagnetic, acoustic, or other device. The courts have not yet addressed whether a communication through company-owned equipment would be considered a "private communication"—this may depend on 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[11] came into force. It applies only to federally regulated industries and organizations that send personal information across provincial and other borders. It creates protections regarding the collection, use, or disclosure of personal information in the course of commercial activity. By 2004, the Act will apply 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 the appropriate monitoring by an employer for Internet use, in particular:

1. identifying and disclosing the purposes for which personal information is collected,
2. obtaining the consent of the individual for collection of personal information,
3. limiting the collection of personal information to that necessary for the purposes identified, and
4. making available to individuals company policies and practices regarding management of personal information.[12]

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 labour legislation, and whether it is part of the private or public sector. The differences in these jurisdictions are too many to deal with here; suffice it to say that, for monitoring policies

[10]R.S.C. ch. C-46 (1985).
[11]S.C. 2000, c. 5.
[12]James G. Knight, *Abuse of the Internet and E-mail*, Address to the University of Guelph—Supervisory Program, 2001.

to be considered reasonable and enforceable, they will have to balance the individual's expectations of privacy and the employer's right to protect sensitive information and assets (including computers and their networks), as well as ensuring that its operations are conducted efficiently and in conformity with the law.

Common sense and established labour relations principles would also suggest that 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 we do not require an employer to post rules against theft before we uphold discipline on that ground, one would not expect arbitrators to demand clear rules against using an office Internet system for transmitting hate literature before we upheld discipline for such conduct.

A recent case dealing with interception of phone calls may signal how e-mails could be treated. A Hindu mission was concerned about theft and unauthorized long distance calls at the mission. As a result, the executive committee decided to tap the phone lines. One of the things it discovered was a series of calls between the mission's married priest and one of its married volunteers. Under pressure, the priest resigned. He and the volunteer then sued for defamation and invasion of their privacy rights under the Quebec Charter of Human Rights and Freedoms. Section 5 of the Quebec Charter provides that "[e]very person has a right to respect for his private life." The Quebec Court of Appeal applied the provincial Charter and the reasoning that has been applied to the Canadian Charter section 8 protections and began its analysis by asking if the persons involved had a reasonable expectation of privacy in the conversations. The court held that because the players in this case were confidants, they had a reasonable expectation of privacy and their conversations were not related to professional matters. They were each awarded monetary damages for violation of their privacy rights.[13] It is clear that the case would have had a different result if the intercepted conversation had revealed discussion related to or detrimental to the defendant's business.

---

[13]*Srivastava v. Hindu Mission of Can.*, 2110-020, full text, in French only, *as reported in* Jeffery Miller, *Off the Record: Workplace Phone Call Protected by Privacy Law?*, LAWYERS WEEKLY, July 6, 2001.

The concept of the "reasonable expectation of privacy" is fundamental to the Canadian approach to electronic surveillance. It is a major factor in the considerations that arbitrators have applied to issues of video surveillance.[14] Other factors that have been applied to the challenge of camera placements in a workplace may be relevant. 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 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 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.[15]

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

> [T]here 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.[16] Both the Ontario Labour

---

[14] *Toronto Transit Comm'n & A.T.U. Local 113 (Russell),* [1998] 88 L.A.C.4th 109 (Shime).
[15] *Lenworth Metal Prods. Ltd. & U.S.W.A. Local 3950,* [1999] 80 L.A.C.4th 426 (Armstrong).
[16] *Thibodeau-Finch Express Inc. & Teamsters Local 880,* [1988] 32 L.A.C. 271 (Burkett).

Relations Board and an interest arbitrator have also expressed serious concern about placement of an "electronic eye" in the workplace.[17]

Unions have long taken the position that camera surveillance is a "despised device for monitoring the workforce."[18] One has to wonder, however, whether there will be somewhat of a change in this perspective. Use of video cameras is now an accepted method of ensuring safety. Anecdotally, I have observed that unions that once challenged the installation of video cameras now welcome them as assisting in maintenance of safety. Cameras now exist in banks, shopping centres, 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 expectation 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 toward surveillance in general.

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 to accept evidence that the arbitrator considers proper, "whether admissible in a court of law or not."

Section 278.5(2) of the Canadian Criminal Code 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:

---

[17]*Purtex Knitting Co. & Canadian Textile & Chem. Union*, [1979] 23 L.A.C.2d 14 (Ellis); *Royalguard Vinal Co.*, [1994] O.L.R.B. Reports Jan. 59.

[18]Richmond, *supra* note 8.

(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[19] that dealt with this issue of whether the employer could seek production of the grievor's personal diary of events in the workplace. The grievor's habitual note-taking during critical events had been one of the grounds for her discharge. Picher acknowledged that a board of arbitration is not a criminal court, but he concluded that arbitrators should consider the Code as an "instructive and useful" guide in the exercise of discretion regarding the admission of evidence. In addition, he applied the Supreme Court of Canada's[20] 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
   a. originate in a confidence,
   b. the confidence must be essential to the relationship in which the communication arises, and
   c. the relationship must be one that 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

[19] *Ontario Power Generation & Power Workers' Union*, [2001] 97 L.A.C.4th 90.
[20] *R. v. O'Conner*, [1995] 4 S.C.R. 411; *M. (A) v. Ryan*, [1977] 1 S.C.R. 157.

   a. 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
   b. 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.

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 the 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;
- 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; and
- 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 affect the integrity of the arbitration process.

Arbitrators will most likely treat the personal notes or journals that an employee may keep in a personal file on their office computer in the same way.

Arbitral Treatment of Internet Use or Abuse by Employees

Overuse of the Internet is being accepted as an employment offence. Regardless of whether policies are in place dictating the amount of permissible time, excessive time spent on nonwork-related Internet exploration is treated as grounds for discipline. Discharges are being upheld where there is accessing of porno-

graphic sites or dishonesty in the course of the investigation.[21] Lesser consequences such as 1-day suspensions are also being accepted.[22] 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 of the employer's ability to monitor the grievor's Internet use after reinstatement.[23] None of these cases questions the employer's right or ability 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 invasion of privacy via the Internet more seriously than the abuse of the Internet itself. An employee of Canadian Pacific used the Internet to send sexually intimate messages to another employee who was his girlfriend, as well as derogatory gossip about a co-worker. In addition, the same employee was party to unauthorized access of yet another employee's computer files.[24] The fact that 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 was considered a mitigating factor. The arbitrator held that, given that the messages to the girlfriend were intended to be confidential even though they amounted to distasteful "electronic graffiti," a "relatively light measure of discipline" would be appropriate. He concluded, however, 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 the 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,

---

[21] *Calgary Reg'l Health Auth. v. Health Science Ass'n of Alta. (Dickinson)*, [1999] AGAA No. 66 (Moreau) (Aug. 24, 1999); *DuPont Canada Inc. v. C.E.P. Local 28*, [2001] 92 L.A.C.4th 261 (Palmer).

[22] *British Columbia Gov't v. B.C. Gov't Servs. Employees Union (Maddison)*, [1998] B.C.C.A.A.A. No. 535 (Kelleher) (Nov. 17, 1988).

[23] *Chronicle Journal v. Thunder Bay Typographical Union Local 44*, [2000] O.L.A.A. No. 575 (Marcotte) (July 27, 2000).

[24] *Canadian Pac. Ltd. & Transp. Communications Union*, Canadian Railway Office of Arbitration, Case No. 2731 (Picher) (May 17, 1996).

than, for example, engaging in idle gossip in a private one-on-one conversation.[25]

In a third railway case,[26] a significant penalty was upheld against an employee for using the e-mail system to obtain answers to a work-related correspondence apprentice course he was taking to further his career. He also corresponded with his friends, even though he was not authorized to use e-mail. This correspondence was described as " not altogether unusual for a 26 year old" and reflecting a "mild case of barracks' humour." The employer had combined the two infractions and discharged the employee. However, the arbitrator concluded that the correspondence was insufficient reason to elevate the discipline to a discharge. The arbitrator refused to agree with the employer that this amounted to "theft" of equipment or resources.

Opening someone else's e-mail, however, even in a system where everyone had been given a default password, was considered to be sufficient grounds for discharge. This was held to be akin to opening personal mail on someone's desk or impersonating the proper user.[27]

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 that someone else was the author. The company's IT staff had little trouble tracing the culprit. His conduct was considered 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 a devastating effect on his reputation in the workplace. The arbitrator called this a "borderline case."[28]

These cases show a respect for the privacy of computer files and illustrate that invasion of that privacy will be treated as a serious employment offence. However, the cases also operate on the

---

[25]*Canadian Pac. Ltd. & Transp. Communications Union*, Canadian Railway Office of Arbitration, Case No. 2732 (Picher) (May 17, 1996).

[26]*Canadian Pac. Ry. Co. & International Bhd. of Elec. Workers*, Canadian Railway Office of Arbitration, Case No. AH-473 (Picher) (Mar. 14, 2000).

[27]*Fraser Valley Reg'l Library & CUPE Local 1698 (Mathews grievance)* (unreported) (Burke, Aug. 31, 2000).

[28]*Westcoast Energy Inc. v. CEP Local 686B*, [1994] 84 L.A.C.4th 185 (Albertini).

assumption that there is really no privacy in the e-mail system. They suggest that users should recognize that what may be intended as private correspondence might well be treated as if they were notes posted on a 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.[29] 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 revealed theft of material from a stock room. The same tape also revealed that the stock room was being used for sexual exploits by two other employees. The criminal defense lawyer argued that since others were prepared to carry on an affair in this stock room, there was a "reasonable expectation" of privacy in that area. Therefore, 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 indicates a reasonable expectation of privacy?

Electronic Pornography

Electronic pornography is treated as a category unto itself. Perhaps because of its taboo nature and some of its illegality, the cases concerning storage, downloading, and distribution of pornography or sexually explicit material do not even discuss issues of privacy. 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, accessing Internet pornography at work may be blamed for creating a poisoned environment and damaging a corporation's reputation.

In one case, a woman was discharged after receiving and distributing material that the company characterized as pornographic.[30]

---

[29] *Insurance Corp. of B.C. & Office & Tech. Employees Union Local 378* (unreported) (Weiler, Jan. 27, 1994).

[30] *Consumers Gas & Communication, Energy & Paperworkers Union* (unreported) (Kirkwood, Aug. 5, 1999).

Management had become aware of the situation after the material entered 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 30-day suspension. The length of 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 of child pornography is a criminal offence. When child pornography is generated by a computer, it is considered a "visual representation" within the meaning of the Criminal Code. Proof of possession will result in a criminal conviction.[31] Proof of possession involves the concepts of knowledge and control. Employers and employees alike are susceptible to conviction if it can be proved that such files are known to be within their control.

A fascinating development in this area involves the defenses that are being raised. In an ongoing case of a community college teacher caught downloading child pornography in a college computer lab setting, the union has raised the employment defense that this person suffers from a mental disorder or disability that requires accommodation to the point of "undue hardship" under the Human Rights Code. The disabilities have been labeled as "Internet addiction" or "pathological Internet use" that expert witnesses are saying should be treated as illnesses rather than as culpable behaviour. The duty to accommodate and the definition of what constitutes a disability have been given a very broad and liberal interpretation in Canada.

---

[31] *R. Weir*, [1998] 213 A.R. 285 (Alta. Ct. Queen's Bench, Feb. 10, 1998).

In a recent case,[32] the grievor 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:

1. that he had a "handicap" within the meaning of the Ontario Human Rights Code,
2. that his viewing of pornography on the Internet at work was causally related to that handicap, and
3. that therefore his termination 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 antidiscrimination provisions of the collective agreement.

On the basis of unchallenged medical evidence, the arbitrator concluded that the grievor suffered from 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." Accordingly, the linkage of his condition to his behaviour caused the arbitrator to reach the following conclusion:

> 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.

Given the grievor's 10-year seniority and the favourable medical prognosis, the arbitrator substituted a 5-day suspension for the discharge. The reinstatement was conditioned on medical evi-

---

[32] *Corporation of the City of London & CUPE Local 101* (unreported) (Marcotte, Oct. 2001).

dence indicating that the grievor was successfully continuing 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 and the application of the traditional concept of using a medical condition as a mitigating factor. It will be interesting to see where this approach may take us.

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 IT policies and practices of the Crown in Right of Ontario (the Crown), the employer of the Ontario civil service, and the Association of Management, Administrative and Professional Crown Employees of Ontario (AMAPCEO). The Crown's IT policy states that "access is intended for government business and ministry or agency approval is required." Under those auspices, the Crown has allegedly prohibited and blocked e-mail communication between AMAPCEO and its members over Crown computer equipment. A complaint was filed by AMAPCEO before the Ontario Labour Relations Board (OLRB) alleging that this amounted to an unfair labour practice by unlawfully interfering in AMAPCEO'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 it had an interest in the outcome of the case in that all the adjudicators at the OLRB are subject to the same IT policies.[33] Further, it was asserted that the IT policies gave the Crown the technical ability and the right to monitor and gain access to the private notes, e-mail, and draft decisions of OLRB members. Therefore, it was asserted that the OLRB did 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.

---

[33] *Crown in Right of Ont. as represented by Management Bd. of Cabinet & Association of Mgmt., Admin. & Prof'l Crown Employees*, O.L.R.B. File 1581-00-U (M.E. Cummings, Alternate Chair, Oct. 1, 2001).

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

> [I]n 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 computerized text files, but it is contrary to its IT policy to scrutinize 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—it has engendered a great deal of controversy. The litigation should itself be recognized as arising in a climate of intense union distrust and animosity against the current Ontario government. However, the case should not be dismissed as relevant only to the political climate of today. One should not underestimate the importance of the fact that adjudicators are being asked to rule not only on the validity of IT usage policies, but also on the implications of their potential abuse by those with the ability to monitor and effectively invade the privacy of all users.

The hearing 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 conduct business on company premises, utilize company bulletin

boards, and use company equipment. Would the same principles apply, or does use 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 employer 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 it 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.

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. 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."[34]

This decision shows a recognition of the unique medium that the Internet provides. It allows for the instantaneous transmission of ideas, which is one of its strengths, but it also discourages the moment of sober second thought that often occurs while we search for an envelope. This leaves the question as to whether the result

---

[34] *O'Neil v. Towers Perrin*, [2001] O.J. No. 3453 (Ontario Superior Court 2119-010, August 28, 2001).

would have been the same if the letter had been sent by post or interoffice memo. Do words really have a different meaning if we have to go to the trouble of finding an envelope and stamp rather than clicking on "send" with a mouse? Wouldn't this have enormous implications on the capacity to contract via e-mail? Could I rescind an offer by saying that I really did not mean what I said in my last e-mail?

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 childrens' bus driver on their bus, and filed complaints with the school board. 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 community's knowledge of them "could undermine her authority as a school bus driver." Her discharge was upheld.[35]

What does this case tell us? Perhaps the lesson is that the advent of the Internet has meant the ease of erasing any semblance of privacy. Further, any actions that are capable of being captured in a form that can be transmitted via technology expose us to the consequences of that public forum.

What Privacy Is Left to the Employee?

Canada's Privacy Commissioner, George Radwanski, speaks 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."

---

[35] *Bader Bus Serv. Ltd. v. Reavely*, [2000] C.L.A.D. No. 648 (Etherington).

> 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.[36]

Radwanski also recognizes, however, 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 (1) necessity, (2) effectiveness, (3) proportionality, and (4) severity. These concepts may well have application in the workplace in terms of assessing the reasonability of any monitoring.

But other realities must be faced. So far, we 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 equip their employees with laptop computers to allow for greater flexibility and productivity. But 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 virtual "broadcast station[s]" that are easily susceptible to infiltration.[37] Where 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 to the market put in question the very existence of the concept.

Conclusion

Canadians are often scorned for failing to be leaders. But Canadian arbitrators are often applauded for being balanced and sensitive to emerging new issues. We follow the philosophy of the Canadian chicken who was asked why she was crossing the road. She answered, "To get to the middle."

We seek to balance employer and employee rights on the issues of Internet use in the modern workplace. But many new issues are

---

[36]George Radwanski, *A New Era of Privacy Protection*, Address to the Treasury Management Association of Canada, 19th Annual Finance & Treasury Management Conference, Oct. 2001.

[37]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.

emerging, and we have just seen the tip of the iceberg in terms of what must be sorted out.

Let me conclude with something to put all of this into a different perspective: The Internet is new, exciting, even mysterious to many. It 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.[38]

[38]Robert Wilensky, *Quotes of the Week*, MAIL ON SUNDAY, Feb. 16, 1997.