ALBERTA'S STATUTORY PRIVACY REGIME AND ITS IMPACT ON THE WORKPLACE

SANDRA M. ANDERSON*

The author describes the tension created by the new privacy legislation between the individual values of personal privacy and the common values of the workplace. There is a detailed discussion of the respective obligations of employers and employees to protect and make accessible personal records held by the employer. The article focuses on various types of employee information, including health information, and discusses in what circumstances they can be disclosed to an employer. Next, the developing impact of the privacy statutes on labour law is surveyed, specifically the rights of unions to obtain employees' personal information. Then the author examines the extent of employee personal information the employer is entitled to have and in what circumstances by surveying three controversial areas: video and other surveillance, drug and alcohol testing and electronic monitoring in the workplace. She concludes that privacy legislation is having a major impact on rights and relationships between employers and employees.

L'auteure décrit la tension, créée par la nouvelle législation sur le respect de la vie privée, entre les valeurs personnelles de la vie privée et les valeurs communes du lieu de travail. Il y a une discussion détaillée sur les obligations respectives des employeurs et des employés de protéger les dossiers personnels gardés par l'employeur et de les rendre accessibles. L'article porte sur divers types de renseignements sur les employés, y compris les renseignements sur la santé, et examine dans quelles circonstances ces renseignements peuvent être communiqués à un employeur. L'auteure analyse ensuite l'effet grandissant des lois sur le respect de la vie privée dans le droit du travail, tout spécialement les droits des syndicats d'obtenir des renseignements personnels sur les employés. L'auteur examine ensuite la portée des renseignements personnels de l'employé que l'employeur peut avoir et dans quelles circonstances, en analysant trois secteurs controversés, à savoir la vidéosurveillance et autres formes de surveillance, les tests de toxicomanie et d'alcoolisme et la surveillance électronique au lieu de travail. Elle conclut que les lois sur le respect de la vie privée ont un très grand effet sur les droits et les relations entre employés et employeurs.

TABLE OF CONTENTS

* B.A. (Duke University), M.A., Ph.D. (Northwestern University), LL.B. (University of Calgary), Partner, Field LLP, Edmonton, Alberta. The author represents clients in relation to several specific issues in this article, but has avoided reference to positions advocated where litigation is ongoing at the time of writing (August 2005).

I. INTRODUCTION

In Alberta, as in the rest of Canada, privacy legislation "opens to employees and former employees a new corridor of interaction with the employer."[1]

It is striking to compare descriptions from our highest Court of the two values that are the subject of this article, privacy and work. In 1987, work was described as a core value in our society:

> Work is one of the most fundamental aspects in a person's life, providing the individual with a means of financial support and, as importantly, a contributory role in society. A person's employment is an essential component of his or her sense of identity, self-worth and emotional well-being. Accordingly, the conditions in which a person works are highly significant in shaping the whole compendium of psychological, emotional and physical elements of a person's dignity and self respect.[2]

Ten years later, privacy was described as:

> An expression of an individual's unique personality or personhood, privacy is grounded on physical and moral autonomy — the freedom to engage in one's own thoughts, actions and decisions....
>
> [There is] the privileged, foundational position of privacy interests in our social and legal culture.[3]

How does one perform "a contributory role in society" by working, while at the same time maintaining one's "physical and moral autonomy"? In other words, are the fundamental values of work and privacy reconcilable?

Courts, arbitrators, Privacy Commissioners, and labour boards are well underway in grappling with the many issues of workplace privacy, aided (or, one might say, bedeviled) by a growing array of privacy statutes, both provincial and federal, which are changing the landscape of labour and employment law.

In the last ten years or so, the battalions of privacy law have marched across Canada, leaving outposts of Privacy Commission offices in Alberta and other provinces to make common cause with federal troops in monitoring rear-guard skirmishes between access to

---

1 Frank Work, "Freedom of Information and the Protection of Privacy" in Kevin Whitaker *et al.*, eds., *Labour Arbitration Yearbook 2001-2002*, vol. 2 (Toronto: Lancaster House, 2002) 61 at 61-62 [Whitaker 2001-2002].

2 *Reference re Public Service Employee Relations Act*, [1987] 1 S.C.R. 313 at 368, Dickson C.J.C.

3 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at paras. 65, 69, LaForest J. in dissent on other grounds [*Dagg*].

information and the protection of privacy. This formidable regime of access and privacy policing has now advanced from the public sector[4] into private sector organizations,[5] leaving a scorched earth of acronyms — *FOIPPA*, *PIPA*, *HIA*, *PIPEDA* — in its wake. Since, in the battle cry issued by Pierre Elliott Trudeau, the state has no business in the bedrooms of the nation, the access and privacy police have not yet fully invaded our homes, but now concentrate on our offices and workplaces, our records and our business practices.

Are we better off for it? The jury is still out, and will be for some time, one suspects, but meanwhile there have been significant changes in the workplace as the result of the plethora of legislative activity concerning the degree to which one's privacy can be invaded or protected. Since, "for most people, work is one of the defining features of their lives" and "any change in a person's employment status is bound to have far-reaching repercussions,"[6] the new emphasis on privacy in the workplace will continue to redefine rights and relationships between employers and their employees in profound ways.

The purpose of this study is not to comb the four corners of the employment battlefield for every trace of carnage, but to focus on a few of the key engagements between the forces that foster access to information in the workplace and those that protect privacy there. It is expected that readers will already have a basic knowledge of the privacy statutes in force in Alberta; if not, there are excellent materials on the websites of the various Privacy Commissions.[7]

II. EMPLOYER-HELD INFORMATION — HOW PRIVATE IS IT?

A. WORKPLACE RECORD-KEEPING[8]

Every organization or business, both in the public and private sectors, is subject to one or other of the privacy statutes because they all hold records in some form that contain information about identifiable persons. No organization can, as before, simply regard any of its records as its "own" to manage as it sees fit.[9] The organization must have a privacy policy that spells out how it will meet its statutory access and privacy obligations and make

---

4 *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25 [*FOIPPA*]; *Health Information Act*, R.S.A. 2000, c. H-5 [*HIA*].

5 *Personal Information Protection Act*, S.A. 2003, c. P-6.5 [*PIPA*]; *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*]. There are privacy statutes in other provinces and at the federal level (*e.g. Privacy Act*, R.S.C. 1985, c. P-21), but their analysis is outside the scope of this article.

6 *Wallace v. United Grain Growers*, [1997] 3 S.C.R. 701 at para. 94 where *Reference re Public Service Employee Relations Act, supra* note 2 at 368 was cited.

7 See *e.g.* Office of the Information and Privacy Commissioner of Alberta, online: <www.oipc.ab.ca>; Alberta Government Personal Information Protection Act, online: <www.pipa.gov.ab.ca>; Office of the Privacy Commissioner of Canada, online: <www.privcom.gc.ca>.

8 As the reader will quickly discern, the analysis in this section applies to statutory obligations with respect to the records of any business or organization, whether as "employer" or otherwise.

9 *PIPA* contains a unique "grandfathering" clause in s. 4(4) for personal information under an organization's control prior to 1 January 2004, so long as that information is used and disclosed for the purposes for which it was collected in the first place. The exception has been of little practical benefit to organizations, at least those which have consulted the author, since it would simply have complicated the objectives of privacy audits and other measures taken to ensure that the management of records as a whole is rationalized to comply with statutory requirements and is internally consistent.

information about its policy and practices available upon request.[10] Its records are subject to disclosure to applicants[11] subject to certain exceptions,[12] to correction by individuals whose personal information they contain[13] and ultimately to investigation and inquiry by the respective federal or the provincial commissioner.[14] An organization's records must be kept securely,[15] retained for appropriate periods to allow full rights of access before destruction[16] and collected, used and disclosed only for a manifest purpose and to the extent consistent with that purpose[17] and with consent from or, in some cases, at least notice to the individuals whose personal information they contain.[18]

It is now clear from many decisions of the federal Privacy Commissioner that employees of businesses subject to *PIPEDA* may not collect personal information from customers that is too intrusive or otherwise unnecessary for the purpose of a business transaction unless the purpose is clearly communicated and the customer consents.[19] Conversely, companies charged with responding to customers must respond to their access requests promptly and

---

10 *PIPA*, *supra* note 5, s. 6; *PIPEDA*, *supra* note 5, s. 24 and Sch. 1, Principles 4.1.4, 4.4.1, 4.8, 4.10.2; there is no equivalent provision in *FOIPPA*.

11 *PIPA*, *ibid.*, ss. 24, 52(2)(a); *PIPEDA*, *ibid.*, s. 5 and Sch. 1, Principle 4.9; *FOIPPA*, *supra* note 4, ss. 2(a), 6(1).

12 See Part IV.B below.

13 *PIPA*, *supra* note 5, s. 25; *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.9.5; *FOIPPA*, *supra* note 4, ss. 36, 37, 37.1.

14 The question of whether an organization or business is subject to federal or provincial privacy legislation and to what degree personal employee information comes within the ambit of *PIPEDA* due to its restriction to collection, use and disclosure of personal information "in the course of commercial activities" (s. 4(1)(b) and s. 2(1)) are questions beyond the scope of this article and can be, in any case, a complex, fact-specific determination.

15 *PIPA*, *supra* note 5, s. 31; *FOIPPA*, *supra* note 4, s. 38; *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.7. Both *FOIPPA*, s. 20(1)(m), and *PIPEDA*, Sch. 1, Principle 4.9, place restrictions on access if the security of the records may be compromised by giving access. What level of security of records is required will vary from organization to organization and will depend in part on the sensitivity of the personal information contained in the records in question.

16 *PIPA*, *ibid.*, ss. 35, 59(1)(c); *PIPEDA*, *ibid.*, s. 8(8), Sch. 1, Principles 4.5, 4.5.2; *FOIPPA*, *ibid.*, ss. 35(b), 92(1)(g); see Violet French & Ari Tenenbaum, "PIPEDA imposes requirements for documents destruction" *The Lawyers Weekly* 24:45 (8 April 2005) 9.

17 *PIPA*, *ibid.*, ss. 1, 11(2), 16(2), 19(2); *PIPEDA*, *ibid.*, ss. 3, 5(3), Sch. 1, Principles 4.2-4.6; *FOIPPA*, *ibid.*, ss. 33, 34(2), 39(4).

18 *PIPA*, *ibid.*, ss. 8(3), 8(4), 13(1), 15(2)(c), 18(2)(c), 21(2)(c); there is no equivalent in *PIPEDA* or *FOIPPA*.

19 See *e.g. PIPEDA* Case Summary #9, "Bank teller writes account number on cheque"; Case Summary #42, "Air Canada allows 1% of aeroplan membership to 'opt out' of information sharing practices"; Case Summary #54, "Couple alleges improper disclosure of telephone records to a third party"; Case Summary #82, "Alleged disclosure of personal information without consent for secondary marketing purposes by a bank"; Case Summary #99, "Personal information improperly disclosed to collection agency"; Case Summary #121, "Bank employee uses customer's information to commit fraud"; Case Summary #139, "Individual claims that bank collected unnecessary information and retained it for too long"; Case Summary #176, "Bank records customer call without consent; refuses to erase tape"; Case Summary #203, "Individual raises concerns about consent clauses on credit card application form"; Case Summary #213, "Bank employee discussed customer's personal information with relatives"; Case Summary #256, "Customer finds bank's collection, use and disclosure of personal information excessive in order to open a personal deposit account, considers bank's purposes vague"; Case Summary #262, "Airline agrees to amend privacy policy"; and Case Summary #277, "Mass mailout results in disclosure of contest entrants e-mail addresses"; all online at: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2005/index2-5_e.asp>.

within the time limits set out in statute for providing access to personal information.[20] At the same time, they must be specially vigilant to ensure that all personal information is kept securely.[21]

Similar issues have arisen under *PIPA*. In the first investigation reports released by Alberta's Commissioner, two large utility companies were found to have collected personal information from their customers which far exceeded their business needs, although one had adequately protected it during transfer to another business.[22]

These obligations in relation to the employer's records do not lie solely with the employer. Presumably because it is primarily an employer's employees who produce the records and are engaged in actual record-keeping in the course of the organization's undertakings, employees are, under *PIPA*, themselves independently and personally liable for breaches of the privacy statutes, while the employer remains liable as well.[23] This opens a new avenue for liability to be spread among employers and employees, in addition to liability any employer may incur vicariously as a result of actions taken by employees acting within the scope and in the course of their duties. Similarly, there is additional exposure to liability for employers when they engage agents, such as benefit and pension providers, office cleaners, payroll administrators and courier services, to handle personal information of their employees and customers, since employers and their agents are equally responsible under *PIPA* for personal information in their custody and control while in the hands of agents or contractors.[24]

B. DISCIPLINE AND RECORD-KEEPING

---

20 *PIPEDA* Case Summary #196, "Company denied customer access to his personal information," online: Office of the Privacy Commissioner of Canada <www.privcom.gc/ca/cf-dc/2003/cf-dc_030801_01_e.asp>; and Case Summary #216, "An airport is accused of not having disclosed all the personal information requested by an employee and of not having retained other personal information," online: Office of the Privacy Commissioner of Canada <www.privcom.gc/ca/cf-dc/2003/cf-dc_030801_07_e.asp>.

21 *FOIPPA*, *supra* note 4, s. 38; *PIPA*, *supra* note 5, s. 34; *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.7; *Report on an Investigation into the Security of Customer Information: Linens 'N Things* (28 January 2005), Investigation # P2005-IR-001, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf>; *Nor-Don Collection Network Inc.* (31 January 2005), Investigation # P2005-IR-002, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf>; *Digital Communications Group Inc.* (3 Feburary 2005), Investigation # P2005-IR-003, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2005_IR_003.pdf>. Although no fines were imposed, the companies were ordered to contact each of their customers to advise them that they had been exposed to identity theft after customer records and receipts had been lost.

22 *Report on the Investigation to Collection, Use and Disclosure of Customer Information: EPCOR* (26 July 2004), Investigation # P2004-IR-001, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2004_IR_001.pdf> [*EPCOR* Investigation Report]; *Report of an Investigation into Disclosure of Customer Information without Consent, Melrose Rural Electrification Association, ATCO Electric and Direct Energy Marketing Limited* (15 October 2004), Investigation # P2004-IR-002, Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2004_IR_002.pdf>.

23 *PIPA*, *supra* note 5, ss. 5(2), 6; *c.f. PIPEDA*, *supra* note 5, Sch. 1, Principle 4.7.4, which requires organizations to make their employees aware of the importance of maintaining the confidentiality of personal information. There is no equivalent provision in *FOIPPA*.

24 *PIPA*, *ibid.*, ss. 5(2), 6; there are no equivalent provisions in *PIPEDA* or *FOIPPA*.

Can an employee be disciplined or terminated for failing to carry out his or her duties in relation to record-keeping or access to and privacy of the employer's records? Not if the employee is attempting to comply with the statute.[25] However, just as it is open to an employer to discipline an employee for failing to follow other policies put in place by the employer, an employee who fails to follow an organization's privacy policy may be at risk of discipline or termination.[26]

It is an employer's right to adopt a policy preserving the confidentiality of the employer's business information and third-party personal information that employees acquire in the course of their employment and to insist that employees follow it.[27] Such a policy is not rendered unreasonable merely by virtue of the fact that it may require explanation and the exercise of judgment in implementing it.[28]

C. EXCEPTIONS TO ACCESSING EMPLOYER-HELD INFORMATION

In contrast to *FOIPPA*, which applies to all records in the custody or under the control of a public body, with certain exceptions,[29] *PIPEDA* and *PIPA* apply to personal information held about identifiable individuals, not to business records in the private sector generally. Therefore, the exceptions to access in *PIPEDA* and *PIPA* are fewer and more narrowly focused on individual interests, in contrast to the broad exceptions to access in *FOIPPA* based on protecting from disclosure records containing confidential commercial, financial, labour relations, or technical information or trade secrets of a third party, tax information, public safety, law enforcement, intergovernmental relations, Cabinet and Treasury Board confidences, drafts and advice from officials, audits and privileged information, *etc.*[30]

---

25 *FOIPPA*, *supra* note 4, s. 91(1); *PIPEDA*, *supra* note 5, s. 27.1; *PIPA*, *ibid.*, s. 58.

26 See *e.g. Manitoba Telephone System (Re)*, [1998] M.G.A.D. No. 35 (Manitoba Grievance Arbitration), where the grievor's termination was upheld for improper monitoring or wiretapping a customer's (the Union's!) telephone line; but in *Alberta Mental Health Board v. United Nurses of Alberta (Dismissal Grievance)*, [2001] A.G.A.A. No. 44 (Alberta Grievance Arbitration), the employee's termination for accessing the employer's computer records to obtain and share information about a former patient was reduced to an eight-month suspension without pay.

27 Examining confidential files, such as medical records, listening in or taping telephone conversations, or accessing other employees' e-mail, or misusing the Internet at work have all resulted in discipline or termination of employment; see Donald J.M. Brown & David M. Beatty, *Canadian Labour Arbitration* (Aurora, Ont.: Canada Law Book, 2005) at 7:3330.

28 *Re Vancouver Island Health Authority and British Columbia Nurses' Union* (2004), 132 L.A.C. (4th) 102. The Union grieved the reasonableness *ab initio* of the employer's privacy policies, not the disciplinary application of it which is still subject to the requirement that there be just cause: *Re Lumber & Sawmill Workers' Union, Local 2537, and KVP Co. Ltd.*, (1965), 16 L.A.C. 73. Nevertheless, the arbitrator's decision is interesting because the policy in question states not only that it incorporates B.C.'s *Freedom of Information and Protection of Privacy Act* (R.S.B.C. 1996, c. 165) but also makes intentional viewing of confidential information that is not necessary to perform an individual's role a breach of confidentiality even if the information is not disclosed to a third party. In addition, a signed confidentiality acknowledgment was made a requirement of the employment or contract/agency relationship and required the employees to have a general understanding of the two policies and the obligations that flowed from them in addition to the potential for discipline for breach of them. This was held not to be an "agreement" with individual employees contrary to the Union's representational rights but a reasonable adjunct of the employer's privacy policies.

29 Set out by category of information primarily in *FOIPPA*, *supra* note 4, s. 4(1).

30 *Ibid.*, ss. 16, 18, 20, 23, 24, 27.

The contrast in the scope and content of the exceptions to access between *FOIPPA* on the one hand and *PIPA* on the other is dramatic when the information sought is not the personal information of the applicant for it. In s. 17 of *FOIPPA*, there is nuanced provision for determining whether disclosure would be prohibited as an unreasonable invasion of a third party's personal privacy, starting with a presumption against disclosure of employment history,[31] financial or medical information, *etc.*, and requiring the public body to consider a number of factors in ultimately determining whether the presumption has been rebutted or not.[32] By contrast, there is a much more sweeping, black-and-white exception to access to employer-held, third-party personal information in s. 24(3) of *PIPA* which gives no discretion to the organization to release it:

> (3) An organization *shall* not provide access to personal information under subsection (1) if
>
> ...
>
> (b) the information would *reveal personal information about another individual*;
>
> (c) the information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his or her identity.[33]

While this exception is softened somewhat by the mandatory severing provision that follows it (s. 24(4)), the result of s. 24(3) is to prevent an organization from providing access to unsevered third-party personal information at all, no matter how reasonable giving access might be, such as when an organization simply wants to return copies of documents to an employee who provided them to the employer in the first place.

III. PERSONAL EMPLOYEE INFORMATION — WHAT IS IT?

The privacy statutes vary in the scope of the information they regulate for access and privacy purposes.[34] All focus on "personal information," defined broadly as information about an identifiable individual.[35] An individual's name, title, business address and telephone number (in other words, one's identity for work purposes) are exceptions to *PIPEDA*'s definition of personal information; otherwise, its provisions apply equally to an employee's personal information as to any other personal information and consent to collect, use and disclose an employee's personal information is required.[36]

---

31 However, *FOIPPA*, *ibid.*, s. 17(1)(e), provides that it is not unreasonable to disclose an employee's classification, salary range, discretionary benefits and employment responsibilities.

32 The reader is referred to *FOIPPA*, *ibid.*, s. 17, as a whole, instead of this abbreviated description.

33 *PIPA*, *supra* note 5, s. 24(3) [emphasis added].

34 *PIPEDA* regulates information collected, used or disclosed in the course of commercial activities by every organization in the federal private sector (*PIPEDA*, *supra* note 5, ss. 4(a)-(b)), while *PIPA* regulates all personal information held by Alberta's private sector organizations (*PIPA*, *ibid.*, s. 4(a)). However, *FOIPPA* regulates all records in the custody or under the control of a public body (*FOIPPA*, *supra* note 4, s. 4(1)).

35 *PIPA*, *ibid.*, s. 1(k); *FOIPPA*, *ibid.*, s. 1(n); *PIPEDA*, *ibid.*, s. 2. While elaborating on the types of information that constitute personal information, *FOIPPA* limits the definition to "*recorded* information about an identifiable individual" [emphasis added].

36 *PIPEDA*, *ibid.*, Sch. 1, Principle 4.3. Consent is on a "sliding scale" of formality, depending on the circumstances and sensitivity of the personal information (Sch. 1, Principles 4.3.4, 4.3.6, 4.3.7). The various forms of consent, express or "opt-in" consent, "opt-out" consent and implied consent are described in "Fact Sheet: Determining the appropriate form of consent under the *Personal Information*

By contrast, *PIPA* is unique in recognizing that the real nature of the employment relationship is not exclusively consensual. It distinguishes personal information and "personal employee information," not only by a similar exception for business contact information,[37] but also by making special, more relaxed provision for the collection, use and disclosure of personal employee information.[38] Personal employee information is defined as

> personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing, or terminating (i) an employment relationship ... but does not include personal information about the individual that is unrelated to that relationship.[39]

For information to be considered personal employee information, the individual in question must be an employee or being recruited as a potential employee, and the collection must be reasonable for the purposes for which it is being collected. *PIPA* contains an expansive definition of "employee" which includes apprentices, volunteers, participants, students, or persons under contract or in an agency relationship with the organization.[40]

With certain exceptions,[41] *PIPA* requires an organization to collect, use and disclose an individual's personal information only with that individual's informed consent.[42] However, if personal information is personal employee information, then the exceptions are broader: *PIPA* permits an employer to collect, use and disclose that information without the employee's consent so long as the purpose for collecting, using or disclosing is explained, notice is given, and reasonable opportunity to refuse consent is afforded the employee.[43] *PIPA* also allows an organization to collect personal employee information and use it or disclose it to another organization without the individual's consent as long as the other organization is also collecting the information for the purpose of recruitment or the individual is an employee of that other organization.[44]

Like *PIPEDA*, *FOIPPA* does not make special provision for "personal employee information," but an individual's employment history is personal information.[45] An employee

---

Protection and Electronic Documents Act," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp> and in "Privacy Annual Report to Parliament 2002-2003," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/information/02_05_e.asp> at 17.

37 *PIPA*, *supra* note 5, ss. 1(a), 4(3)(d).

38 *Ibid.*, ss. 15(1), 18(1), 21(1).

39 *Ibid.*, s. 1(j).

40 *Ibid.*, s. 1(e). *FOIPPA*, *supra* note 4, s. 1(e) definition is similarly broad.

41 Such as the "reasonableness," determined on an objective standard, of collecting, using or disclosing the information, or the information is publicly available, or its availability is regulated by an enactment of Canada or Alberta, *etc.* See *PIPA*, *ibid.*, ss. 14, 17, 20.

42 *PIPA*, *ibid.*, ss. 7-8.

43 *Ibid.*, ss. 8(3), 15(2), 18(2), 21(2).

44 *Ibid.*, ss. 15(1)(b) and (3); compare ss. 18 and 21. This may be especially useful with respect to reference letters, which appear to qualify as personal employee information under *PIPA*; by contrast, under *PIPEDA*, an employer must obtain specific consent in order to check references regarding a potential employee.

45 *FOIPPA*, *supra* note 4, s. 1(n)(vii); *PIPEDA*, *supra* note 5, s. 4(1)(b).

of a public body includes an appointee, volunteer, student, contractor or agent.[46] Certain work products of employees are exempted from disclosure under *FOIPPA*.[47]

Although not defined as such, personal employee information is generally protected from disclosure under *FOIPPA*. When provided in confidence, personal information related to an employee's suitability or qualification for employment or evaluations may be withheld, as may consultations or deliberations concerning employees.[48] There is a presumption that disclosing employment information to an applicant for access would be an unreasonable invasion of a person's privacy if the information is related to the other person's employment history.[49] Disclosure of an employee's personal information to the employee's union requires that employee's written consent.[50] Conversely, personal information may be disclosed to an employee of a public body only if it is necessary to the employee's performance of his or her duties.[51]

This multiplicity of approaches to employees' personal information in *PIPEDA*, *PIPA* and *FOIPPA* is a first sign that it will take a great deal of time before it is clear with any real degree of certainty what effect the privacy statutes in force in Alberta will have in the workplace. The ambivalence to the protection of employees' personal information is not surprising. After all, employment involves an intricate exchange of services for money within a multifaceted and frank relationship between employer and employee. The employment relationship cannot permit an employee to maintain an autonomous relationship compatible in all respects with privacy, "grounded on physical and moral autonomy — the freedom to engage in one's own thoughts, actions and decisions."[52] In every employment relationship, and with varying degrees of complexity, employers need access to their employees' information to monitor, assess and maintain the employment relationship, while employees need access to employer-held information to do their jobs or protect their own rights.

IV. EMPLOYEES' PERSONAL INFORMATION — HOW ACCESSIBLE IS IT TO OTHERS?

An employer typically has a great deal of information about each of its employees, ranging from information provided at hiring, including references, background checks, security clearances, including a criminal record check, credit bureau report, personal address and telephone number, ongoing surveillance results, company benefit plan information, potentially including medical and counselling records with the most personal details about the employee's health, marriage and family. Can others, such as fellow employees, an outside applicant, benefits insurers, service providers, or the union, access that information?

---

46 *FOIPPA*, *ibid.*, s. 1(e).

47 The exceptions include teaching materials and research information of a post-secondary educational body (*FOIPPA*, *ibid.*, ss. 4(1)(h)(i) and 4(1)(i)). A public body may also refuse to disclose information obtained by an employee's research if the disclosure would deny priority of publication (*ibid.*, s. 25(1)(d)).

48 *Ibid.*, ss. 19(1), 24(1).

49 *Ibid.*, s. 17(4)(d).

50 *Ibid.*, s. 40(1)(o); see discussion under Part IV.B below.

51 *Ibid.*, s. 40(1)(h).

52 *Dagg*, *supra* note 3 at para. 65.

Much personal employee information, in particular that as revealed between benefit insurer and employer, is collected indirectly, not, as for example, *PIPA* and *FOIPPA* require, directly from the employee himself or herself.[53] However, even under *PIPA*, an employer may collect, use and disclose personal employee information indirectly and without consent if it relates to the employment relationship or is required for recruiting purposes and is reasonable for the purpose of establishing, maintaining or terminating the employment relationship.[54] It would be difficult to argue that an employer does not require or is not entitled to certain medical information to provide health-related benefits or to accommodate the employee who returns to work.

The employer's main obligation is to inform employees beforehand about the purposes for which the personal employee information is being collected, used and disclosed and to ensure those purposes are reasonable.[55] Notice is not required if the collection, use or disclosure is reasonable for an investigation or legal proceeding or is authorized by law.[56]

Certain types of routine employee information have been the subject of particular scrutiny by the Privacy Commissioners. Unless the evaluations were provided in confidence, evaluations about an applicant for access may have to be disclosed to him or her because they are the personal information of the applicant, not the evaluator,[57] but *PIPA* mandates the opposite result, as s. 24(3), quoted above, makes clear. Letters of reference have been both ordered disclosed to[58] and withheld from[59] employees who are the subject of them. A complaint file held by a public body will not be released to an applicant for access, unless the materials can be severed and limited to those which contain the applicant's own personal information.[60]

---

53 *PIPA*, *supra* note 5, s. 7(1)(b); *FOIPPA*, *supra* note 4, ss. 34(1), (2); implied in *PIPEDA*, *supra* note 5, Sch. 1, Principles 4.2.3, 4.4, 4.4.1.

54 *PIPA*, *ibid.*, ss. 15(2)(a)-(b), 18(2)(a)-(b), 21(2)(a)-(b).

55 *Ibid.*, ss. 11, 15(2)(c), 16, 18(2)(c), 19, 21(2)(c).

56 *Ibid.*, s. 14(b), (d), 17(b), (d), 20(b), (m).

57 *FOIPPA*, *supra* note 4, ss. 1(n)(viii), 19; see *French v. Dalhousie University* (2003), 212 N.S.R. (2d) 215, 2003 NSCA 16. *PIPEDA* is silent on the issue.

58 *University of Alberta* (21 March 2001), Order 2000-029, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/2000-029.pdf> (student reference letters seen by several decision makers; no unreasonable invasion of privacy since applicant asked referees to write letters as well).

59 *University of Calgary* (10 October 2003), Order F2002-027, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2002-027.pdf> (refusal upheld since confidential reference was to determine the applicant's suitability for employment and it came within s. 19(1)); *Grant MacEwen College* (16 July 2003), Order F2003-008, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2003-008.pdf> (no duty to disclose 2002 reference letter when former employee had been terminated in 1996).

60 *The Board of School Trustees of School District No. 68 (Nanaimo-Ladysmith)* (16 February 2004), Order 04-04, online: Office of the Information and Privacy Commissioner for British Columbia <www.oipc.bc.ca/orders/order04-04.pdf>; but see *University of Alberta* (28 June 2005), Order F 2003-009, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2003-009.pdf>.

An employee who seeks access to his or her personal information withheld by an employer may run up against the principle that the employer may withhold such information if the employer has taken *no job action* as the result of that information.[61]

The same principle applies if there is *an insufficient connection* between the private materials and the public body employer, such as the personal diary of a school principal containing his account of work-related events (investigations, complaints and allegations concerning the applicant for access) but never used for a work-related purpose or intended to form part of the official records of his employer.[62] On the other hand, if an employee, such as a school counsellor, has made personal notes in the course of fulfilling his or her employment responsibilities and the notes were relied upon in preparation of periodic reports, they are not merely the employee's, but are, rather, under the employer's control and produceable to the applicant whose personal information they are, unless a statutory exception applies.[63] The real test is whether an employee's records, even if they record work-related information, are made on his or her own time and with his or her own materials, and were made without being required or requested by the employer to do so. When that is the case, they will not be within the employer's custody and control so as to be available to an applicant for access.[64]

PIPEDA does not go so far. When a terminated former employee of a trucking company was denied access to his records, the complainant believed that the employer's general manager was withholding information about him by keeping it on a home computer, despite the manager's sworn statements to the contrary. While the suspicion might have been correct, the federal Privacy Commissioner ruled that he did not have the power to enter a dwelling place for purposes of an investigation, so that he was limited to ruling that the former employee had received all the information to which he was entitled.[65]

---

61 *University of Alberta* (21 January 2003), Order F2002-030R, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2002-030R.pdf> (reconsideration after judicial review); *University of Alberta v. Pylypiuk* (2002), 310 A.R. 300, 2002 ABQB 22 (the author was counsel for the University). See also *PIPEDA* Case Summary #60 "Airport employee demands access to personal information from airline," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc_020719_e.asp>.

62 *Inquiry Re: A decision of School District No. 58 (Nicola-Similkameen) on the custody or control of a retired school principal's diary* (13 July 1998), Order No. 247-1998, online: Office of the Information and Privacy Commissioner of British Columbia <http://142.31.70.39/orders/1998/Order247.html>.

63 *Neilson v. British Columbia (Information and Privacy Commissioner)*, [1998] B.C.J. No. 1640 (QL), affirming *Inquiry Re: A request for access to school counsellor's notes in School District No. 2 (Cranbrook)* (23 August 1996), Order No. 115-1996, online: Office of the Information and Privacy Commissioner for British Columbia <www.oipc.bc.ca/orders/1996/Order115.html>. The employing School Board asserted the notes were under its custody and control, and the counsellor testified that the notes were taken for her use only, as an *aide mémoire* in counselling children and should, therefore, be withheld under s. 19(1)(a) (Alberta's *FOIPPA*, *supra* note 4, s. 18(1)(a)). The B.C. Commissioner and the Court disagreed, since the notes were relied upon in preparation of periodic reports, and the counsellor was an employee, not an independent contractor.

64 *Ministry of the Environment* (20 February 1998), Final Order P-1532, online: Information and Privacy Commissioner of Ontario <www.ipc.on.ca>.

65 *PIPEDA* Case Summary #179 "Trucking company accused of refusing form employee's access request," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030708_e.asp>.

While Principle 4.9 of Schedule 1 of *PIPEDA* requires disclosure to an individual, including an employee, of his or her personal information, s. 9(3)(d) provides that an organization need not provide access if the information was generated in the course of a formal dispute resolution process. This has recently been held to be true in Alberta also for personal information relating to a complaint the applicant for access had made against another employee.[66]

This limitation on access in internal public body resolution processes does not pertain to a file generated in the course of a human rights investigation.[67]

While an employer may collect employees' personal information, such as SIN numbers, there is less scope for use and disclosure by employers of that information unless there is good reason.[68] Even the release of identifying information without the name of the employee may be impermissible.[69] In a recent decision of Alberta's Information and Privacy Commissioner,[70] two law firms and their clients were chastised for having posted on a website the home addresses and SIN numbers of employees of a business which was being acquired by another. Despite s. 22 of *PIPA*, which permits disclosure of personal information for the purpose of determining whether to proceed with the transaction, such information was not necessary to the transaction. The Commissioner gave examples of personal employee information that could be relevant and disclosable in the course of the sale or acquisition of a business: description of functions and jobs, salary levels, pension and stock purchase plans, outstanding litigation with employees and union bargaining units.[71]

---

66 *University of Alberta* (28 June 2005), Order F 2003-009, *supra* note 60. The author was counsel for the University.

67 *PIPEDA* Case Summary #88 "Former telco employee denied access to certain employment file information," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2002/cf-dc_021031_e.asp>.

68 *EPCOR* Investigation Report, *supra* note 22; Office of the Information & Privacy Commissioner of Alberta & Office of the Information & Privacy Commissioner for British Columbia, "Use of Social Insurance Numbers by Private Sector Organizations" (April 2005), online: Office of the Information and Privacy Commissioner for B.C. <www.oipc.org/sector_private/public_info/SINtipsFinalApr5.pdf>; *PIPEDA* Case Summary #69, "Employee objects to company's use of social insurance numbers on form," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2002/cf-dc_020904_1_e.asp>; Case Summary #242, "Individual objects to temporarily assigned workers handling payroll information," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_031204_D6_e.asp>; Case Summary #145, "Alleged disclosure of personal information to a third party without consent," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030401_2_e.asp> (if a management company is managing an organization's employees under an agreement which allows for sharing of employee information, the sharing of personnel files is not in contravention of *PIPEDA*).

69 *Report on Investigation into Complaint Regarding Disclosure of Personal Information Northern Alberta Institute of Technology* (27 May 2004), Investigation Report F2004-IR-001, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/Report.pdf>.

70 *Report of an Investigation into the Disclosure of Persons Information During the course of a Business Transaction, Builders Energy Services Ltd., Stikeman Elliott LLP, Shtabsky & Tussman LLP and Remote Wireline Services Ltd.* (12 July 2005), Investigation Report P2005-IR-005, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2005_IR_005.pdf>.

71 *Ibid.* at 7.

Complaints of inadequate security for employees' personal information have also been upheld as well-founded.[72]

Improper disclosure of personal information by an employer may be the subject of a successful complaint to the Privacy Commissioner; for example, in one case, members of Niagara Falls city council disclosed details of the grievor's lack of skills in water testing allegedly to embarrass him because he was married to one of the councillors who was a vocal critic of the city's water quality. The arbitrator found that there is an implied reciprocal obligation in a collective agreement not to disclose confidential information, similar to the common law duty impressed on employees of loyalty to the employer. This reciprocal obligation rests on an express or implied provision in a collective agreement that it will be subject to provincial law, including the province's privacy statutes.[73] After the Ontario Commissioner's mediator found that the information had been improperly disclosed, but failed to provide a personal remedy, the union asked the arbitrator to provide the grievor with a remedy based on the "tort aspect" of the claim; that is, the harm which the disclosure and publication of confidential information from the employee's personnel file inflicted on him. The employer disputed that the privacy statute in question was employment related, but the arbitrator found that the grievance was nevertheless arbitrable.[74]

A. EMPLOYEES' HEALTH INFORMATION

Health information is, along with a person's financial information, the most sensitive of personal information. This is recognized in the special statutory regimes for health information when it is in the hands of a "custodian," primarily, hospitals, nursing homes, doctors and other medical service providers.[75] Obviously, not all employers are "custodians," and even custodians have other information not regulated by *HIA* as health services, such as employment information.[76] However, "health information" under *HIA* does include written information about profession, job classification, employment status, number of years of practice and employer.[77] While similar restrictions on its collection, use and disclosure exist in *HIA* as in *PIPA*, *PIPA* makes it clear that it does not apply to health information to which *HIA* applies.[78] This means that employees' health information not held by "custodian" employers is subject to *PIPA*, and it should only be collected, used and disclosed with the employee's consent or with proper notification of purpose and opportunity to withdraw consent, as already described above. A custodian may not release individually identifying

---

72 See *e.g. PIPEDA* Case Summary #23 "Employee objects to employer's use of bank account number of pay statement," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_01_e.asp>.

73 *Canadian Union of Public Employees, Local 133 v. Niagara Falls (City) (Iaonnoni Grievance)*, [2005] O.L.A.A. No. 228 at paras. 25, 30, 37-43, 45, 53, 68, 82, 85-90, 92, 104-108 (QL).

74 It should be kept in mind that the *Ontario Labour Relations Act*, S.O. 1995, c. 1, Sch. A. contained at the time s. 48(12)(j), which gave Ontario arbitrators a power not expressed in Alberta's *Labour Relations Code*, R.S.A. 2000, c. L-1; namely, the power "to interpret and apply human rights and other employment-related statutes, despite any conflict between those statutes and the terms of the collective agreement."

75 *HIA*, *supra* note 4, ss. 1(1)(f), 5.

76 *Ibid.*, s. 1(2).

77 *Ibid.*, ss. 1(1)(k), (o)(xiv) – (xviii); see also ss. 22, 27, 34, *etc.*

78 *PIPA*, *supra* note 5, s. 4(3)(f), as am. by *Personal Information Protection Amendment Act*, S.A. 2005, c. 29, s. 2(a).

health information to the employer of the individual without consent, unless the custodian believes on reasonable grounds that the disclosure will avert or minimize an imminent danger to the health or safety of any person,[79] a situation that does not present itself often in the course of an employment relationship. An employee can keep track of what release there is of his or her health information by requesting to see the logs describing the circumstances of the release.[80]

In the federal arena, *PIPEDA* also makes special provision for "personal health information,"[81] and the federal Commissioner has elaborated on the sensitivity of such information.[82]

The Workers' Compensation Board (WCB) takes the position that, since s. 20(c) of *PIPA* permits disclosure of personal information to a public body such as itself when a statute of Alberta or Canada authorizes or requires it, employers (and physicians) continue to be required to provide details of injury and accidents, as well as other employer-held personal and employment information.[83] This may turn out not to be the case, since s. 4(6) of *PIPA* provides that *PIPA* prevails in cases of inconsistency or conflict with another statute, unless that statute or a *PIPA* regulation expressly provides that the other statute prevails notwithstanding *PIPA*.[84] In public sector decisions under *FOIPPA*, the Commissioner has ordered the WCB to disclose personal information to an applicant and to adhere to the requirements for correcting information.[85] However, it has also been held that "a person who applies for benefits necessarily lowers his or her expectation of privacy in respect of his or her medical records," justifying the mandate of the WCB to examine the legitimacy of a claim.[86]

The enforcement of the *Occupational Health and Safety Act*[87] may reveal considerable health information about an injured worker, and a recent regulation enacted under the *Insurance Act*[88] requires individuals to authorize the release of any relevant health information and to be assessed by certified examiners in order to determine whether a minor

---

79 *HIA*, *supra* note 4, s. 35(1)(m).

80 *Ibid.*, s. 41.

81 Defined specially in *PIPEDA*, *supra* note 5, s. 2, but mentioned again only in Sch. 1, Principle 4.3.5.

82 *PIPEDA* Case Summary #120, "Employer's practice of collecting personal medical information to support a transfer request deemed appropriate," online: Officer of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030217_3_e.asp>; Case Summary #191, "Company's collection and disclosure of employee sick leave information," online: Officer of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030711_e.asp>.

83 See *e.g. Workers' Compensation Act*, R.S.A. 2000, c. W-15, ss. 18, 33, 34, 37, 103, 105, 108, 109. See "Privacy Statement," online: WCB <www.wcb.ab.ca/privacy/>.

84 None of *FOIPPA*, *PIPA*, *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003 [*PIPA Regulation*] or the *Workers' Compensation Act* itself makes the express provision required to defeat *PIPA* paramountcy.

85 *Workers' Compensation Board* (26 May 1998), Order 98-010, online: Office of the Information and Privacy Comissioner of Alberta <www.oipc.ab.ca/ims/client/upload/98-010.pdf>; *Workers' Compensation Board* (6 March 2001), Order 2001-009, online: Office of the Information and Privacy Comissioner of Alberta <www.oipc.ab.ca/ims/client/upload/2001-009.pdf>.

86 *Simons v. Prince Edward Island (Workers' Compensation Board)* (2000), 188 Nfld. & P.E.I.R. 13, 2000 PESCAD 15 at para. 6 (C.A.).

87 R.S.A. 2000, c. O-2.

88 R.S.A. 2000, c. I-3.

injury occurred.[89] Along with expanding electronic health information networks (and their risk of unauthorized disclosure),[90] the Government of Alberta has also established a committee to conduct a focused review of *HIA*-related issues, such as extending *HIA* to the private sector, disclosing health information to police services in the case of suspected criminal activity, and reporting when a prescription reveals an attempt to commit an offence.[91]

It is understandable, then, that how much health information is in the hands of the employer and what the employer does with it is of grave concern to employees.

It would be difficult to argue that an employer does not require or is not entitled to certain medical information for the purpose of determining whether an employee is ready to return to work after a medical leave, since the employer is entitled to know whether the employee is able to work and to work safely without putting himself or herself and others at risk. An employer is also obligated to explore alternate ways of doing a job for purposes of adjusting the workplace to accommodate a disabled employee. In order to discharge that obligation, the employer is entitled to have the medical information necessary for it to determine the employee's functional restrictions and to determine how to deal with the situation, to the point of undue hardship for the employer.[92]

Another purpose for an employee's medical information is to determine suitability for a safety-sensitive job. If the medical evidence is incomplete or unsatisfactory or conflicting, the employer may legitimately ask for more, especially if there is a compelling business reason, such as safety, for doing so. Generally, what is necessary is the least amount of medical information sufficient for the purpose for which it is required.[93] This should be especially true when an employer demands medical information about other members of an employee's family for purposes of group benefits coverage.

Since there is a "special privacy interest" in an employee's medical information into which an employer may not intrude, questions on a medical certificate required for extended or partial medical leave about an employee applicant's functional and cognitive abilities and

---

89 *Minor Injury Regulation*, Alta. Reg. 123/2004.

90 A real risk, as it turns out, since in March 2005, it was discovered that there was a large-scale disappearance of Albertans' health information while in transit between two government facilities. The Commissioner has investigated the problem (*Report on Investigation into Missing Computer Tape Containing Health Information, Alberta Health and Wellness* (30 June 2005), Investigation Report H2005-IR-001, online: Office of the Information and Privacy Comissioner of Alberta <www.oipc.ab.ca/ims/client/upload/H2005_IR_001.pdf>); see James Baxter, "Errant tapes contained medical, pension info" *Edmonton Journal* (30 March 2005) A3.

91 See Review of the Health Information Act, online: <www.assembly.ab.ca/HIAReview/index.htm>.

92 James A. D'Andrea, *Illness and Disability in the Workplace: How to Navigate Through the Legal Minefield*, looseleaf (Aurora, Ont.: Canada Law Book, 1995); and Andrew Sims, ed., "Reasonable Accommodation in the Workplace: Dealing with Injury and Disability Workshop" (University of Calgary, 6 June 2001).

93 See Brown & Beatty, *supra* note 27 at 7:6142.

whether there were any non-medical barriers to recovery were prohibited as being beyond what is reasonably required from a physician on a routine, general medical certificate.[94]

However, in the context of accommodating an employee's return to work, at least a minimum of medical evidence is required. In the absence of such evidence, the duty to accommodate does not extend to preserve an employee's employment status on a mere speculative expectation that he or she might be able to return to work in some capacity in the future and the employer of such an employee is justified in terminating for non-culpable absenteeism. When such an employee refused to provide the medical evidence on the basis that it would violate his right to privacy, one arbitrator noted:

> I note in passing that the Employer was not in a position to require the Grievor to breach his right of privacy with respect to medical information. Its remedy [dismissal] was the one it selected. That is, it was entitled to include the failure to provide medical information in the facts it relied on to support its conclusion with respect to the Grievor's ability to attend at work in the foreseeable future.
>
> ...
>
> The Employer established that the Grievor had failed to attend work and, following repeated inquiries, had been unable to provide the Employer with facts with respect to when and if he would be able to report for work. In short, the Grievor was unable to refute the projection dictated by the facts with respect to his continuing inability to work in the foreseeable future. On that basis the grievance is dismissed.[95]

In other words, an employee's interests in work and privacy are to be balanced against the employer's obligation to have a safe workplace and its right to have employees who can be expected to attend work.[96] The regulations under *FOIPPA* underline this by permitting a public body to disclose information relating to the mental or physical health of an individual to a medical or other expert for an opinion on whether disclosure of the information would reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health.[97]

Employers may also take some comfort from one decision[98] in which the federal Commissioner dismissed a complaint that the employer had collected more personal information than was necessary. In that case, the telecommunications employer administered its policy on extended sick leave by having employees sign consent to specific purposes, such as considerations of eligibility for benefits and establishment of fitness for work. Employees also signed forms (a) authorizing their physicians to disclose to the employer's occupational health therapists medical information related to the employee's illness or

---

94 *British Columbia Teachers' Federation v. British Columbia Public School Employers' Association*, [2004] B.C.C.A.A.A. No. 177 (B.C.) (QL); see *Re St. James-Assiniboia School Division No. 2 and St. James-Assiniboia Teachers' Association No. 2* (2004), 131 L.A.C. (4th) 313 (Man.) (stringent onus on employer in seeking additional medical disclosure during six-week post-partum period).

95 *Kelfor Industries Ltd. v. Industrial Wood and Allied Woodworkers Union of Canada, Local 1-3567 (Anderson Grievance)*, [2003] B.C.C.A.A.A. No. 214 at paras. 58, 63-64 (B.C.) (QL).

96 See also *Re City of Brampton and Canadian Union of Public Employees (Krejci)* (2003), 122 L.A.C. (4th) 445 (Ont.); *Re Board of Health for the Hastings and Prince Edward Counties Health Unit and Candian Union of Public Employees, Local 3314* (2004), 125 L.A.C. (4th) 272 (Ont.).

97 See *Freedom of Information and Protection of Privacy Regulation*, Alta. Reg. 200/1995, s. 5.

98 *PIPEDA* Case Summary #120, *supra* note 82.

inability to work; (b) authorizing their physicians to discuss the employees directly with the employer; and (c) authorizing their physicians to disclose information about the employee's medical condition, treatment and prognosis. The employer was also found to have acted reasonably by keeping personal health information in a separate file, passing on to managers and others outside the disclosure framework the above disclosed information only to the extent that it related to the abilities and limitations of the employees and by having sufficient security protections in place.

In a more recent decision, the federal Commissioner went further, dismissing a complaint that a self-insuring employer's health unit screened the complainant's files and then disclosed background details about previous grievances and difficulties in the workplace to an independent medical examiner who then determined that the complainant was not fully disabled. The employer terminated her disability benefits. The Commissioner found that the complainant's previous absences and other background material were directly relevant to the employer's determination of the complainant's ability to return to work and her eligibility for continuing disability benefits and that the complainant should reasonably have been aware of that when she attended the independent medical examination. To require express consent of an employee in such circumstances before releasing the information about performance would impose an unreasonable burden on organizations or might lead to situations where the organization's legitimate purposes are not met.[99]

Ultimately, two major issues arise: if an employer demands access to medical information with respect to an employee's condition and the employee refuses, to what extent can the employee be compelled to account for his or her absence from work? Does the refusal constitute cause for discipline? After all, the duty to accommodate encompasses a duty on the employee (and union) to provide sufficient medical information to the employer to assess the extent and type of accommodation required.[100]

Employers should re-examine their disclosure obligations under existing insurance plans. In considering disclosure between employers and insurers with respect to employees, employers should remember that it would be prudent to treat employees as though they were third parties to insurance plans and that in any event no agreement between insurer and employer can prevail against any of *PIPA*, *PIPEDA* or *HIA*, since "any waiver or release given of the rights, benefits or protections provided under this Act is against public policy and void."[101]

In the further context of benefits insurers, employers may increase the risk of consequences to employees (and the risk to themselves of being sued by them) if they insist, or agree with the benefits insurer's insistence, on medical examination or treatment of their employees by health care providers of the employer's or benefit insurer's choosing, rather

---

99 *PIPEDA* Case Summary #284, "Use and disclosure of health information considered appropriate, but access request was mishandled," online: Office of the Privacy Commissioner of Canada <www.privcom.gc/ca/cf-dc/2004/cf-dc_041130_e.asp>.

100 See *Re Rosewood Manor and Hospital Employees' Union, Local 180* (1990), 15 L.A.C. (4th) 395 (B.C.); *Health Employers' Assn. of British Columbia (M.S.A. General Hospital) v. Hospital Employees' Union (Steenbergen Grievance)*, [2000] B.C.C.A.A.A. No. 12 (B.C.) (QL).

101 *PIPA*, *supra* note 5, s. 4(7); *c.f. PIPEDA*, *supra* note 5, s. 4(3); and *HIA*, *supra* note 4, s. 4.

than taking the opinion of the employee's physicians; this is the so-called "independent" medical examination that employees consider slanted toward the employer's or insurer's interests. As a patient, the employee is in a vulnerable position, and the employer runs a risk of contributing to foreseeable harm from any misconduct or negligence on the part of the health care provider.[102]

On infrequent occasions, unions may be able to consent to organizations having access to their members' personal health information by virtue of the fact that they may be the individual's "authorized representative" under *PIPEDA* or *HIA*.[103] Conversely, an employee may not be coerced into giving up her privacy rights by an employer seeking information to substantiate a termination, even when the employee was being discharged for improper use of sick leave.[104]

B. EMPLOYEES' PERSONAL INFORMATION — ACCESS BY UNIONS, ARBITRATORS AND LABOUR BOARDS

One of the most vexing of new issues at the intersection of the labour relations and privacy sectors is the reconciliation between the privacy statutes, with their emphasis on the personal information, privacy and access rights of individuals, and traditional collective labour rights, where unions act as the agents of their members in codifying terms and conditions of employment in collective agreements and in taking on the employer by way of grievances and other job action. On the one hand, employers are uncertain as to the extent of disclosure they may or must provide to the unions which represent their employees.[105] On the other, unions face the double dilemma of (a) meeting resistance from employers to the disclosure to their unions of their employees' personal information as the result of the privacy statutes and (b) fulfilling their new statutory obligations, like any other organization in the private sector, to protect privacy of personal information and personal employee information while giving applicants access to their personal information.

PIPA makes no provision for union involvement in the collection, use or disclosure of an employee's personal information, except that an individual may be represented at an inquiry held by the Commissioner by a lawyer or agent.[106] Access to personal information is an individual matter[107] and, as referred to previously, an organization is prohibited from providing access to information that would reveal personal information about another individual.

Section 24(3)(b) of *PIPA* imposes a restriction on an agent, or bargaining agent, of the applicant to access the applicant's information, as the applicant would be "another individual" vis-à-vis the union's representative. However, there is one exception: the *PIPA*

---

102 *T.W. v. Seo* (2003), 126 A.W.C.S. (3d) 271 (Ont. Sup. Ct. J.).

103 *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.3.6; *HIA*, *supra* note 4, s. 104(1)(i).

104 *Re Canada Post Corporation and Canadian Union of Postal Workers* (2001), 100 L.A.C. (4th) 39 (Can.).

105 It is now well established that basic contact information, such as employees' home addresses and telephone numbers must be disclosed; see *infra* note 123.

106 *PIPA*, *supra* note 5, s. 50(3)(a), similar to *FOIPPA*, *supra* note 4, ss. 69(5), 74.5(5).

107 See *e.g. PIPA*, *ibid.*, s. 24.

Regulation[108] also permits a union, as a private sector organization, to collect, use and disclose personal information without the consent of the individual if the collection, use or disclosure is necessary to comply with a collective agreement referred to in s. 128 of the *Labour Relations Code*,[109] an exception that further erodes the privacy of employees in the private sector in relation to their employer.

PIPEDA is silent on the subject of unions and bargaining agents. The federal Commissioner has settled complaints of employees that their unions received their personal information without their consent by having the employers adjust their databases to eliminate information going to the unions without the specific consent of the employees.[110] The federal Commissioner also found that an employee who stated that she acted on her own in submitting an access request to her employer, then complained when the employer copied her union representative with its response to her, had not given implied consent to the disclosure to the union, nor was such disclosure a purpose a reasonable person would consider appropriate in the circumstances, as required by s. 5(3) of *PIPEDA*.[111]

In another decision of the federal Commissioner, the complainant was summoned as a witness in a grievance by another employee, where she was confronted with her own performance appraisals during cross-examination. She complained that her personal information was disclosed without her consent and the disclosure was improper. Only the arbitrator, the complainant and the lawyer representing the grievor's union had copies. The federal Commissioner found that while *PIPEDA*, Principle 4.3 of Schedule 1 stipulates that the knowledge and consent of the individual are required for disclosure, s. 7(3)(c) permits such disclosure if it is required to comply with a subpoena issued or an order made by a person with jurisdiction to compel production. Since under the *Canada Labour Code*[112] arbitrators have such power, the acceptance of the appraisals into evidence at the hearing was an "order" within the meaning of s. 7(3)(c). Had that not been the case, then counsel would have to seek permission from the witness and obtain an order from the arbitrator for the disclosure.[113]

In this area of the demarcation between labour relations and privacy, *FOIPPA* appears to be the most complex of the acronymic statutes. There is a mandatory exemption from disclosure by the public body of information that would reveal

> labour relations ... information of a third party....that is supplied explicitly or implicitly in confidence, and the disclosure of which could reasonably be expected to...interfere significantly with the negotiating position

---

108 *PIPA Regulation*, *supra* note 84, s. 19(a).

109 *Supra* note 74.

110 *PIPEDA* Settled Case Summary #7, "Company eliminates excessive information from database," online: Officer of the Privacy Commissioner of Canada <www.privcom.gc.ca/ser/2004/s_040227_02_e.asp>; *PIPEDA* Settled Case Summary #4, "Company amends employee list it sends to union," online: Office of the Privacy Comissioner of Canada <www.privcom.gc.ca/ser/2004/s_041105_e.asp>.

111 *PIPEDA* Case Summary #20, "Employer sends third parties copies of response to employee's access requests," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_04_e.asp>.

112 R.S.C. 1985, c. L-2, as. am.

113 *PIPEDA* Case Summary #198, "Employer accused of wrongful disclosure," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030801_03_e.asp>.

> of the third party ... or reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.[114]

The Commissioner has held that a public body's information is not the "labour relations information of a *third party*," but the exemption can include information of a management person or information about union members and information in relation to grievances; it is not limited to "collective" labour relations.[115] Moreover, the union as a "group of persons" might be a third party, as described in *FOIPPA*, s. 1(1)(r), when acting in a representative capacity for its member or members, so that the employer may be able to claim the exemption on the basis that the union is the third party.[116]

There is provision in *FOIPPA* for disclosure of personal information to a representative of the employee's bargaining agent but only when the bargaining agent "has been authorized in writing by the employee the information is about to make an inquiry."[117] The fact that the bargaining agent, like anyone else, requires the consent of the individual before the public body is authorized to disclose that individual's personal information is significant, as is the restriction to the activity of *making an inquiry*.[118] That is, the representative of the bargaining agent cannot obtain the benefit of access to a member's personal information under this provision for another purpose, such as pursuing a grievance. It indicates that the concept of the union bargaining agent as the exclusive representative of its members, enshrined in the *Labour Relations Code*,[119] is as absent from *FOIPPA* as it is from *PIPA* or *PIPEDA*. The Commissioner has emphasized that, in relation to a union's representative rights, the right of access is an individual one:

> A union member cannot assume that a representative of the union will be extended recognition as his or her agent on an access request. Similarly, a union representative is not entitled to make an access request on behalf of an employee. Section 84(1)(c) [now section 84(1)(f)] of the Act prescribes a procedure for

---

114 *FOIPPA*, *supra* note 4, ss. 16(1)(a)(ii), 16(b), 16(c)(i), (iv).

115 *University of Calgary* (20 September 2000), Order 2000-003, at paras. 99-100, 105-109, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/2000-003.pdf> (applicant seeking report of a mediator called in to resolve the grievance; record need not be disclosed). The Commissioner made it clear in paras. 95-99 that he was revisiting and expanding the conclusion he had reached in *Alberta Labour Relations Board* (21 December 1999), Order 99-030, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/imsclient/99-030.pdf> that "labour relations information" is information about the relations between management and employees.

116 *University of Calgary*, Order 2000-003, *ibid.* at para. 112.

117 *FOIPPA*, *supra* note 4, s. 40(1)(o); this is consistent with the right of an applicant to be represented by an agent during an inquiry by the Commissioner (*FOIPPA*, *ibid.*, ss. 69(1), 74.5(5)). Section 40(1)(o) does not diminish the fact that union members still have a right to personal privacy, as the B.C. Court of Appeal has stated about the B.C. equivalent of s. 40(1)(o) (*Canadian Office and Professional Employees' Union, Local 378 v. Coast Mountain Bus Co.*, [2005] B.C.J. No. 2655, 2005 BCCA 604 at para. 68 (QL) [*Coast Mountain* CA].

118 Similarly, a union cannot rely on the factors set out in s. 17(5) of *FOIPPA*, *ibid.*, for determining whether a disclosure of personal information would constitute an unreasonable invasion of a third party's personal privacy set, specifically s. 17(5)(c): "the personal information is relevant to a fair determination of the applicant's rights," if there is no access request under *FOIPPA* in the first place; in other words, filing a grievance does not trigger the inquiry under s. 17 (*Coast Mountain* CA, *ibid.* at paras. 47-49).

119 *Supra* note 74, ss. 12(3)(l), (o), 21(1), 29(1), 32, 40(1), (3), 59(1), 61(1), 128(1), 144, 151(d).

> appointing agents, and unless that procedure has been followed a union official is simply an outsider, locked out by the privacy protection provisions of the statute.[120]

This approach is reflected in one of the Commissioner's Orders:

> In my view, the Faculty Association's exclusive authority to represent the Applicant in matters set out in the collective agreement does not prevent the Applicant from making an access request under the Act or for asking for a review of the University's refusal to provide access. Furthermore, the Act contains its own scheme for representation under the Act. The Applicant would have to have given written authority under section 79(1)(e) of the Act for the Faculty Association to represent the Applicant under the Act.[121]

Even where a collective agreement provided explicitly for disclosure of particular information, in one case copies of fee-for-service appointment letters of instructors who were not members of the SAIT Faculty Association, the Commissioner did not rely on the collective agreement to order disclosure, but on the fact that SAIT could not succeed in bringing itself within the disclosure sections of *FOIPPA* on which it was relying because the letters were not "supplied to" SAIT by the fee-for-service instructors for the purpose of negotiations so as to fit within s. 16(1)(c)(2), but were, rather, contracts to supply services to SAIT within the meaning of s. 17(2)(f), thus justifying disclosure. Despite what the collective agreement said, the information in issue was the personal information of the third-party fee-for-service instructors.[122]

Labour relations boards, as might be expected, start from a different perspective on disclosure and privacy, one informed by the rights of unions, as the bargaining agents of their members, to have the information they require to carry out their representational responsibilities. After a spate of attempts by employers to withhold information based on concern not to run afoul of the new privacy legislation, a variety of boards have held that the employers were interfering in the unions' right to represent the employees, and that a union is entitled, at the very least, to obtain from the employer employee names, addresses and phone numbers,[123] especially where there is a background labour dispute, such as a pending strike vote, and no sound business reason for refusing the disclosure.[124] In one case at the

---

120 Work, *supra* note 1 at 62.

121 *University of Calgary*, Order 2000-003, *supra* note 115 at para. 115.

122 *Southern Alberta Institute of Technology* (27 April 2005), Order F2004-014, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2004-014.pdf> at paras. 1, 15-17, 20, but see paras. 49-50.

123 *Re Economic Development Edmonton*, [2002] Alta. L.R.B.R. 161 (ALRB), application for a stay denied, [2002] Alta. L.R.B.R. 193, 2002 ABQB 13590; *Re Regional Health Authorities 1, 2, 3, 4, 5, 6, 7, 8 and 9*, [2003] Alta. L.R.B.R. LD-062 (ALRB), reconsideration refused, [2003] Alta. L.R.B.R. 405, judicial review denied; *Communications, Energy and Paperworkers Union of Canada Local 707 v. Alberta (Labour Relations Board)* (2004), 351 A.R. 267, 2004 ABQB 63; *Ottawa-Carleton District School Board*, [2001] O.L.R.D. No. 4575 (OLRB); *Re Governor and Company of Adventurers of England Trading into Hudson's Bay*, [2004] B.C.L.R.B.D. No. 227; *Re P. Sun's Enterprises (Vancouver) Ltd.*, [2003] B.C.L.R.B.D. No. 301; *Public Service Alliance of Canada and Treasury Board*, [1996] C.P.S.S.R.B. No. 30 (CPSSRB); *Ontario (Alcohol and Gaming Commission)*, [2002] O.L.R.D. No. 120 (OLRB). Unions have been found to have improperly withheld records from their members as well, such as in *Re Stone*, [2005] A.L.R.B.D. No. 49 (Alta.) (duty of fair representation complaint).

124 *Millcroft Inn Ltd.*, [2000] O.L.R.D. No. 2581 (Ont.); *Re Economic Development Edmonton*, *ibid.* (first collective agreement); *Re P. Sun's Enterprises (Vancouver) Ltd.*, *ibid.* at para. 23.

federal level, an arbitrator pointed to the "balancing" principle cited in s. 3 as its purpose and found that *PIPEDA* does not bar the employer from providing home addresses and telephone numbers of its employees to the union.[125] In some of the cases, the privacy statutes were not clearly argued, however.[126] In others, a sense of "fairness" weighed in favour of disclosure, in that if the employer already had access to the employees' personal information it was refusing to disclose to the union, there was no reason why the union, as the equal bargaining partner with the employer, should not also have it.[127]

Moreover, the power of labour relations boards and arbitrators to compel attendance of witnesses and to compel production[128] must be considered. The privacy statutes provide that they are not to be applied to limit the information available by law to a party to a legal proceeding and may be disclosed for the purpose of complying with a subpoena, warrant or order made by a court, person or body having jurisdiction to compel production.[129] Since the production must be relevant to the legal proceeding before such an order will go, the fact that disclosure provisions in a collective agreement must now be read in a manner consistent with applicable privacy legislation is already having a limiting effect on disclosure orders; that is, where disclosure is ordered, it is more frequently subject to strict conditions to ensure that only the minimum amount of information is disclosed.[130] A further question is whether the paramountcy or "quasi-constitutional" status of the privacy statutes[131] must be taken into account by courts and tribunals in making their orders to compel production of personal information which otherwise would not be produceable under privacy legislation. To date, these powers to compel production have tended to be interpreted in accordance with previous practice by the tribunals themselves,[132] but with some questioning about the impact of the statutes on disclosure obligations in collective agreements.[133]

---

125 *Re Via Rail Canada Inc. and Canadian Auto Workers, National Council 4000* (2003), 116 L.A.C. (4th) 407 (Can.).

126 In *Re P. Sun Enterprises (Vancouver) Ltd.*, *supra* note 123 at para. 31, the B.C. Labour Relations Board could not even identify which statute the employer was invoking to avoid the disclosure.

127 *Re Economic Development Edmonton*, *supra* note 123 at para. 27; *Millcroft Inn Ltd.*, *supra* note 124.

128 *Labour Relations Code*, *supra* note 74, ss. 14(2), 143(2).

129 *PIPA*, *supra* note 5, ss. 4(5)(b), 20(c); *PIPEDA*, *supra* note 5, s. 7(3)(c); *FOIPPA*, *supra* note 4, ss. 3(c), (d), 40(1)(g).

130 *Coast Mountain* CA, *supra* note 117 at paras. 53, 70-71, 73-74.

131 *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, 2002 SCC 53 at paras. 24-25; *Eastmond v. Canadian Pacific Railway* (2004), 254 F.T.R. 169, 2004 FC 852 at para. 100 (F.C.T.D.) [*Eastmond*].

132 See *e.g. Alberta Mental Health Board v. United Nurses of Alberta*, *supra* note 26; *Re Government of the Province of Alberta and Alberta Union of Provincial Employees* (1998), 83 L.A.C. (4th) 278 (Alta.); but see *Re Economic Development Edmonton*, *supra* note 123 at paras. 10, 29 where the Alberta Labour Relations Board instead approached the matter from the perspective of *FOIPPA*.

133 *Coast Mountain Bus Co. v. Canadian Office and Professional Employees Union, Local 378*, [2005] B.C.C.A.A.A. No.86 [*Coast Mountain* Arbitration], rev'd on other grounds by *Coast Mountain* CA, *supra* note 117; *Southern Alberta Insitute of Technology v. SAIT Academic Faculty Association (Contract Grievance)*, [2002] A.G.A.A. No. 55 at para. 36 (QL).

By contrast and in keeping with the paramountcy provisions of *FOIPPA*,[134] the Commissioner has treated the Labour Relations Board as just another public body subject to *FOIPPA*.[135]

These different perspectives do not resolve the issue of jurisdiction. Several cases have held that labour arbitrators and labour relations boards have jurisdiction to determine questions about privacy and personal information if those questions flow from the employment relationship. For example, in *Re Vancouver Hospital and Health Sciences Centre and British Columbia Nurses Union*,[136] a British Columbia arbitrator relied on the *Weber* analysis[137] to find that the essential character of the dispute (a grievance regarding an allegedly inappropriate and defamatory reference) fell within the ambit of the collective agreement. In *Re Economic Development Edmonton*,[138] the Alberta Labour Relations Board held that it was obliged to consider a request for information under the *Labour Relations Code* and that the *FOIPPA* provisions regarding requests for information do not deprive the Labour Relations Board of the jurisdiction to determine whether employee information should be disclosed to a union.[139] Similarly, in *Ottawa-Carleton District School Board*,[140] the Ontario Labour Relations Board concluded that regardless of whether the union had another means of obtaining information the employer said would breach the employees' privacy rights to disclose, the union was still entitled to come to the Board for relief if a provision of the *Labour Relations Act* had been violated. In that decision as well, the Ontario Labour Relations Board distinguished the ruling of the Ontario Information and Privacy Commissioner in a parallel case[141] for failing to appreciate the labour relations significance of the union's statutory role as agent and representative of the employees in a bargaining unit when he rejected the union's application for information about its members.

Based on the foregoing and on the principle that an arbitrator has broad jurisdiction to fashion a remedy,[142] it appears that arbitrators and labour relations boards remain ready and

---

134 *FOIPPA*, *supra* note 4, s. 5. There is no provision, at least as yet, in the *Labour Relations Code*, *supra* note 74, that it prevails despite *FOIPPA* or *PIPA*, as is necessary to defeat the paramountcy of *FOIPPA* and *PIPA*.

135 *Alberta Labour Relations Board*, Order 99-030, *supra* note 115.

136 (2000), 87 L.A.C. (4th) 205 (B.C.).

137 *Weber v. Ontario Hydro*, [1995] 2 S.C.R. 929 [*Weber*], which adopted an exclusive jurisdiction model arising from the mandatory arbitration clauses in the *Ontario Labour Relations Act* (*supra* note 74) in which arbitration ousts the Court's jurisdiction to hear a civil action if the gist of the factual dispute between the parties expressly or inferentially arises out of the collective agreement.

138 *Supra* note 123 at para. 20.

139 However, where the disclosure issue is essentially one of interpretation and application of the collective agreement, rather than a matter of statutory proportions, the Alberta Labour Relations Board has declined jurisdiction and referred the issue to the arbitrator (*NASA v. University of Alberta* [2005], letter decision, 22 August 2005) (the author was counsel for the University).

140 *Supra* note 123.

141 *Ibid.* at para. 11. In para. 18, the Privacy Commissioner was criticized for "fail[ing] to appreciate the significance of the union's statutory role as agent and representative of the employees in a bargaining unit." The decision under the gun is *Wellington County Board of Education* (9 March 1993), Order M-96, online: Ontario Information and Privacy Commissioner <www.ipc.on.ca/index.html>, in which it was held that the union had no legal interest in the proceedings, and that was relevant to whether the information (home telephone numbers) should be disclosed to it.

142 *Parry Sound (District) Social Services Administration Board v. Ontario Public Service Employees Union, Local 324 (O.P.S.E.U.)*, [2003] 2 S.C.R. 157, 2003 SCC 42.

willing to exercise the broad jurisdictional powers accorded to them by the Supreme Court of Canada in *Weber*, including jurisdiction over disputes with privacy overtones, as long as a sufficient employment-related nexus exists. Moreover, the Federal Court has held that neither the Court nor the federal Privacy Commissioner had jurisdiction to deal with a privacy complaint brought under *PIPEDA* since the issues were related to the complainant's work and arose under the collective agreement.[143]

However, the Federal Court has addressed the jurisdictional relationship between *PIPEDA* and the *Canada Labour Code*,[144] concluding that a complaint that the employer violated *PIPEDA* by using workplace surveillance cameras which collected the employee's personal information without his consent did not arise from the collective agreement and was not arbitrable on the *Weber* principle, specifically rejecting its exclusive jurisdiction model.[145] There was no reason to think that unionized workers subject to the *Canada Labour Code* were excluded from *PIPEDA*'s scope.[146] Consistent with the paramountcy provisions discussed already, the Court emphasized the importance of *PIPEDA*, in a conclusion with implications for the application of all the privacy statutes:

> I have no hesitation in classifying PIPEDA as a fundamental law of Canada just as the Supreme Court of Canada ruled the Federal Privacy Act enjoyed quasi-constitutional status ... (*Lavigne v. Canada*, [2002] 2 S.C.R. 773, at paragraphs 24 and 25).[147]

The *Weber* principle applies more clearly to arbitrators whose jurisdiction flows from the collective agreement. To the extent that a collective agreement contains provisions which impact on disclosure or privacy issues, an arbitrator will certainly be able to decide them. However, in a case in which the disclosure provisions in the collective agreement were impermissibly broad under the applicable privacy statute, an arbitrator has ruled that the union's access must be limited so as not to violate the protections set out in B.C.'s *FOIPPA* concerning personal information.[148] This approach is consistent with the principle of interpreting a collective agreement in a manner consistent with the *Charter*[149] or human rights legislation and is even more appropriate in light of the paramountcy provisions in *FOIPPA* and *PIPA*.[150]

---

143 *L'Écuyer v. Aéroports de Montréal* (2004), 327 N.R. 387, 2004 FCA 237, aff'g (2003), 233 F.T.R. 234, 2003 FCT 573 (QL).

144 *Supra* note 112.

145 *Eastmond*, *supra* note 131 at para. 92.

146 *Ibid.* at para. 99.

147 *Ibid.* at para. 100. The B.C. Privacy Commissioner referred to this case in his discussion of his jurisdiction in his first ruling under B.C.'s *PIPA*, dated 24 March 2005, concerning personal information of members of B.C. Nurses' Union who receive long-term disability benefits.

148 *Coast Mountain* CA, *supra* note 117 at paras. 70-71, 73-75, rev'g on other grounds *Coast Mountain* Arbitration, *supra* note 133 at para. 58 (job posting policy grievance). See also *University of British Columbia v. C.U.P.E., Local 116*, [2005] B.C.C.A.A.A. No. 166 (QL).

149 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [*Charter*].

150 To the extent that privacy statutes may limit production in such a way as to violate the principles of fundamental justice and the right to a fair hearing, the restrictions in the statutes may eventually be subject to a *Charter* challenge; see the discussion by Arbitrator Innes Christie in *PEI Union of Public Sector Employees v. Provincial Health Services Authority* [2005] P.E.I.L.A.A. No. 3 (QL) concerning the prohibitions on disclosure under the PEI *Mental Health Act*, R.S.P.E.I. 1988, c. M-6.1.

It is not yet possible in Alberta to determine with any degree of certainty that jurisdictional disputes between the Commissioner and labour tribunals over access and disclosure issues will necessarily always be resolved in favour of the latter. This is in part due to the fact that both *PIPA* and *FOIPPA* provide that they prevail over inconsistent or conflicting provisions of another enactment unless that other enactment or regulation expressly provides that it prevails notwithstanding *PIPA* or *FOIPPA*, as the case may be.

The Privacy Commissioners are alive to these issues. As David Loukidelis, B.C.'s Information & Privacy Commissioner said:

> Simply put, it serves no one's interests for there to be different rules depending on whether an individual or union complains to a privacy commissioner or instead lodges a grievance and proceeds to arbitration — or both.
>
> The reasons why it's in no one's interest to have different rules depending on whether you go to a privacy commissioner or a labour arbitrator are obvious and familiar. To my mind, it's regrettable, if not downright objectionable in principle, to have different rules and outcomes regarding the same subject-matter just because you go to one forum or another. It's just not good public policy for this to happen without a compelling reason. And it's a waste of time and money to slug it out in more than one forum if, by contrast, it should be possible to resolve the matter using the same principles in either forum. Consistency of rules would discourage, though certainly not eliminate, forum-shopping as between labour arbitrators and privacy commissioners.[151]

This is a welcome invitation to a truce which may yet be elusive. At some point, there will need to be common ground established between the interests of the union in gaining access to personal information of its members and others, on the one hand, and the obligations of the employer and the employees' privacy rights on the other. The truce may take the form of orders that limit production to the union of documents suitably severed to comply with *FOIPPA* or *PIPA*, or that grant full production, but with restrictions on circulation within the union or return of all copies after their use at arbitration is over,[152] or a combination of both.

V. EMPLOYEES' PERSONAL INFORMATION — HOW MUCH IS THE EMPLOYER ENTITLED TO OBTAIN?

The privacy statutes make it clear that not only does an employee have the right to see his or her own personnel file, including letters of reference written about the employee,[153] but that right extends to correcting inaccurate information held on the file, except for opinions

---

151 David Loukidelis, "Arbitrators & Privacy Commissioners — Why They Should Listen to Each Other" (lecture presented to the *Insight* Conference in Calgary on "Privacy Laws & Effective Workplace Investigations," May 2004).

152 See *Re Manitoba Liquor Control Commission and Manitoba Government Employees' Union (Campbell)* (2002), 114 L.A.C. (4th) 436 (Man.) (job selection grievance; safeguards on production ordered).

153 In *University of Alberta* (21 March 2001), Order 2000-029, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/2000-029.pdf>, the Commissioner determined that letters of reference written in support of a student's admission to a graduate program should be released to the student, since they affected the student's career opportunities.

on the file about the employee,[154] which may be withheld from the employee if such opinions were provided in confidence.[155] If for no other reason than to check the accuracy of information, an employee should from time to time ask to see his or her personnel file. Nevertheless, the real obligation is on the employer to collect personal information that is necessary for its stated purpose, to collect it by lawful means, and to inform its employees what it collects from them, why it collects it and what it does with it.[156]

But what is the extent of personal information an employer is entitled to obtain from or about its employees?

> People expect to have some privacy at work, even if they are on their employer's premises and using the employer's equipment. At the same time, it's normal that working for someone will mean giving up some privacy. Employers need basic information about their employees for things like pay and benefits, and they have to be able to ensure that work is being done efficiently and safely.
>
> But the possibilities for infringing on privacy are greater than ever before. Psychological tests, web-browsing records, video surveillance, keystroke monitoring, genetic testing: the information an employer can have about employees is limitless.[157]

It has been held, sensibly, that the more a workplace rule infringes on an employee's right to privacy and the greater the infringement on privacy away from the workplace, the more the burden of proof shifts to the employer to justify the rule as reasonable.[158] In the world of burgeoning methods of intruding on privacy, workplace privacy is under particular assault from video surveillance, drug and alcohol testing, outsourcing and electronic monitoring.

A. SURVEILLANCE

Undoubtedly, the most frequently fought privacy-sensitive issue involves surveillance and monitoring of employees.

> [E]mployee surveillance ... can be understood to be an intrusive inquiry into the private realm of the employee, just as much as a physical search, a drug or alcohol test, a medical exam or the search of a locker or coverall pockets.... The type of information being sought is usually not of any concern to the employer in the normal course of business and is understood generally to be within the realm of the employee's private life. Absent a special or unusual concern (for example a suspicion of theft or sick leave abuse), an employer

---

154 *FOIPPA*, *supra* note 4, ss. 36-37; *PIPA*, *supra* note 5, s. 25; *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.9.5. See *Grant MacEwan College* (11 August 2004), Order F2003-019, online: Office of the Information Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2003-019.pdf> (no requirement to correct professional opinions about the applicant, but College required to properly link the records with the correction request).

155 *FOIPPA*, *ibid.*, s. 19; there is no equivalent in *PIPA* or *PIPEDA*.

156 The federal Commissioner has posted a useful guide entitled "Fact Sheet: Privacy in the Workplace," online: Officer of the Privacy Commissioner of Canada <www.privcom.gc.ca/fs-fi/02_05_d_17_e.asp>.

157 *Ibid.*

158 *Re Finning International Inc. and International Association of Machinists & Aerospace Workers, Local 99* (2004), 135 L.A.C. (4th) 335 at 359 (Alta.) (compelling production of a driver's extract unreasonable, except where necessary for the employer's auto insurance policy).

would not be interested in what an employee carries in his or her pockets, whether they are in good health or what they might be doing when standing in front of their home when not at work.[159]

Generally speaking, it is difficult to bring workplace video surveillance into line with privacy legislation. However, *PIPA* may permit surveillance without consent if the means used are demonstrably necessary to solve a problem of fraud, theft, debt, *etc.* or to investigate whether there has been a breach of a collective agreement or employment contract.[160] There are similar provisions in *PIPEDA* and *FOIPPA*.[161] *FOIPPA*'s provisions for disclosure are more numerous than those for collection, and it emphasizes that the collection should be directly from the individual the information is about.[162] None of the provisions deals explicitly with surveillance.

Even if the employer can demonstrate that the surveillance has been conducted in accordance with those exceptions, however, such surveillance has the potential to capture personal information outside the ostensible purpose of the surveillance. In order to have a chance to withstand challenge, an employer must have consent or must notify the employees at the outset of the purpose for the surveillance, must have a reasonable rationale for the surveillance, and must limit collection to information that is directly related to that rationale and to the employment relationship of the individual concerned.

Since surveillance, especially video surveillance, is a drastic intrusion into employees' personal privacy, and is contrary to the statutory expectation that personal information will be collected from the individual himself or herself,[163] it is expected that the notification and consent provisions in *PIPA* will be applied strictly against the employer to curb unnecessary or overintrusive surveillance practices, as arbitrators have previously done. Employers should ask themselves whether their surveillance is reasonable, using the following test adopted by the federal Commissioner:[164]

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

---

159 *Re Securicor Cash Services and Teamsters, Local 419 (Mehta)* (2004), 125 L.A.C. (4th) 129 at 138-39 (Can.).

160 *PIPA*, *supra* note 5, ss. 14(d)(i), 17(d), (j), 20(f)(i), (n); *PIPA Regulation*, *supra* note 84, ss. 19(a), (b).

161 *PIPEDA*, *supra* note 5, Sch. 1, Principle 4.3; *FOIPPA*, *supra* note 4, s. 33, *c.f.* ss. 40(k)(i), (q), (x).

162 Compare *FOIPPA*, *ibid.*, s. 40 (disclosure) with ss. 33-34 (collection).

163 *PIPA*, *supra* note 5, s. 7(1)(b); *FOIPPA*, *ibid.*, ss. 34(1), (2); implied in *PIPEDA*, *supra* note 5, Sch. 1, Principles 4.2.3, 4.4, 4.4.1.

164 *PIPEDA* Case Summary #114, "Employee objects to company's use of digital video surveillance cameras," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp>; *c.f. PIPEDA* Case Summary #1, "Video surveillance activities in a public place," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2001/cf-dc_010615_e.asp>. In the former, a railway company instituted surveillance cameras in public workplace areas to reduce theft, but since the problem was a potential one, the surveillance contravened *PIPEDA*. In the latter case, surveillance cameras were mounted on a Yellowknife street for commercial purposes, which was without question found to be inconsistent with the privacy rights of the passers-by.

This test is similar to that set out in the early, but leading case of *Re Doman Forest Products*,[165] in which, in the context of the *Privacy Act*,[166] Arbitrator Vickers was considering the admissibility of videotape surveillance evidence where the employer alleged that an employee had abused sick leave. He required the employer to demonstrate the need for such measures and to show that the measures were reasonable in the circumstances. Balancing of employer and employee interests and the reasonableness of the surveillance in relation to the means adopted have long dictated whether videotape surveillance evidence is admissible for purposes of arbitral review of discipline or termination of an employee.[167] Where the video evidence was conducted reasonably, it will be admitted even if it was being used for a purpose (discipline) other than that for which it was collected (security of the employer's store).[168] If a person initiates a lawsuit against a doctor for professional negligence, a videotape made by the doctor of the patient for impeachment purposes is admissible at trial and is not a contravention of the patient's privacy and the principles of *PIPEDA* because it was the patient herself who put the degree of her injury in issue and impliedly consented to the breach of her privacy by the videotaping.[169]

This "reasonableness" test for admissibility of video surveillance evidence imposes a stricter standard on the employer than the "relevance" test.[170] As one arbitrator concluded, it may skew the results:

> Since I am asked to make the assessment of admissibility without having the videotapes tendered before me, there is a risk that I might not fully understand their context, relationship to the relevant events and the extent of the intrusion upon the Grievor's privacy interest, all of which may be important to the ultimate determination of the reasonableness of the Company's conduct. For that reason it is my view that the 'no plausible basis' standard for assessing reasonableness is appropriate at this preliminary stage, but its application can only result in a finding as to whether the Company *prima facie* had a reasonable basis for

---

165 *Re Doman Forest Products Ltd. New Westminster Division and International Woodworkers, Local 1-357* (1990), 13 L.A.C. (4th) 275 (B.C.). The evidence was ruled inadmissible, consistent with *Charter* values, because the employer had not proven a deceitful WCB claim against a longtime employee with an unblemished disciplinary record and had not approached the employee directly with its concern [*Re Doman Forest Products*].

166 R.S.B.C. 1996, c. 373.

167 *Centre for Addiction and Mental Health v. Ontario Public Service Employees Union (Cann Grievance)*, [2004] O.L.A.A. No. 457 at para. 54 (QL); *Ainsworth Lumber Co. (Savona Division) v. United Steelworkers of America, Local 1-417 (Brooks Grievance)*, [2005] B.C.C.A.A.A. No. 73 (QL) (use of private investigation firm, absence of dishonesty, failure to ask grievor for information: surveillance unreasonable); *Re Ebco Metal Finishing Ltd. and International Association of Bridge, Structural, Ornamental & Reinforcing IronWorkers, Shopmens' Local 712* (2004), 134 L.A.C. (4th) 372 (B.C.) (arbitration process would be brought into disrepute if unreasonable surreptitious video evidence were admitted when found contrary to *PIPA*'s provision that it be "reasonable for an investigation" and "reasonable for managing or terminating an employment relationship"). See also Brown & Beatty, *supra* note 27 at 3:4203.

168 *Ontario Liquor Boards Employees' Union v. Ontario (Liquor Control Board) (Goncalves Grievance)*, [2005] O.G.S.B.A. No. 31 at para. 27 (Ont.) (QL).

169 *Ferenczy v. MCI Medical Clinics* (2004), 70 O.R. (3d) 277 (Sup. Ct. J.).

170 The distinction is discussed in *Re Prestressed Systems Inc. and Labourers' International Union of North America, Local 625 (Roberts)* (2005), 137 L.A.C. (4th) 193 (Ont.) beginning at 207.

conducting the surveillance. A higher standard of review at this juncture might unfairly cut off the opportunity for the proposed evidence to be assessed in proper context.[171]

Surveillance outside of work hours and off the employer's premises will be especially difficult for the employer to justify unless there is a relevant connection with the employer's legitimate business interests,[172] such as a suspected abuse of sick leave[173] or the exceptional value of the property the employer has in its custody.[174] However, introducing a sick leave policy designed to cut down on absences which changed the previous call-in-sick "honour" system to one where management followed up on absentees with an inquiring telephone call has been held to be reasonable and not, as the union alleged, contrary to the collective agreement, which was silent on procedures for employees to report being on sick leave.[175]

The privacy statutes have not changed the landscape very much in relation to the approach to video surveillance,[176] but they should be taken into account.[177] For example, in one of the first cases to consider the topic under *PIPEDA*, the CPR's installation of digital cameras in its Toronto railyard was upheld as reasonable given CPR's security and investigation needs.[178] The federal Commissioner has upheld video surveillance where there was a problem with damage to company property, the cameras were trained only at access points to the workplace, storage of the recordings was for a limited duration, the union had agreed to the installation, and there was no intent to use surveillance to monitor productivity.[179] There was a different outcome where a company used the zoom capacity to determine that two employees had being going off-site during working hours, since the company did not

---

171 *Re McKesson Canada and Teamsters Chemical, Energy and Allied Workers Union, Local 424 (Trinh)* (2004), 136 L.A.C. (4th) 102 at 125 (Ont.) (surveillance conducted in public places for suspected abuse of sick leave *prima facie* admissible); see Thomas Jolliffe, "Privacy and Surveillance: Balancing the Interests An Arbitrator's Perspective" in Kevin Whitaker *et al.*, eds., *Labour Arbitration Yearbook 1999-2000*, vol. 2 (Toronto: Lancaster House, 2000) 91 [Whitaker 1999-2000]; Gordon Meurin, "Privacy and Surveillance: Balancing the Interests A Management Perspective" in Whitaker 1999-2000, *ibid.* at 105; John Carpenter, "Privacy and Surveillance: Balancing the Interests A Union Perspective" in Whitaker 1999-2000 *ibid.* at 113.

172 *Re Centre for Addiction and Mental Health and Ontario Public Service Employees Union* (2004), 131 L.A.C. (4th) 97 (Ont.).

173 *Re Grey Bruce Health Services and Ontario Public Service Employees Union* (2004), 131 L.A.C. (4th) 193 (Ont.); *Re Johnson Matthey Ltd. and United Steelworkers of America, Local 9046 (Murray)* (2004), 131 L.A.C. (4th) 193 (Ont.).

174 *Re Glenbow-Alberta Institute and Canadian Union of Public Employees, Local 1645* (1988), 3 L.A.C. (4th) 127 (Alta.).

175 *Re City of Kanata and City of Kanata Professional Firefighters Association* (28 February 1996). Similarly, bag and parcel inspections have been held not to be a substantial violation of personal privacy in the circumstances (*Re Petro-Canada and Communications, Energy and Paperworkers Union of Canada, Local 593* (2004), 132 L.A.C. (4th) 422 (Ont.)).

176 As noted expressly by Arbitrator Munroe in *Pope & Talbot Ltd. v. Pulp, Paper and Woodworkers of Canada, Local No. 8* (2003), 123 L.A.C. (4th) 115 at 125 (B.C.), referring to the *Personal Information Protection Act*, S.B.C. 2003, c. 63.

177 In a lengthy judicial review of an arbitral decision, Clackson J. held that the decision was wrong in concluding that the *Charter* did not apply to the issue of the admissibility of surreptitious surveillance evidence, but was correct in that there was no expectation of privacy, on the facts or in common law, so that no *Charter* remedy was available. There was no reference to *FOIPPA* at all in the analysis (*Amalgamated Transit Union, Local 569 v. City of Edmonton* (2004), 124 L.A.C. (4th) 225 (Alta. Q.B.)).

178 *Eastmond, supra* note 131.

179 *PIPEDA* Case Summary #264 "Video cameras and swipe cards in the workplace," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_e.asp>.

demonstrate that unauthorized absences had previously been a problem either with these two or with other employees and did not try other, less intrusive means to manage the matter.[180] If an employer has tried less intrusive means, such as providing a rehabilitation program, making attempts to accommodate or trying to get up-to-date medical information without success, yet still has well-founded concern about an employee's absences and veracity, then even hiring a private investigation firm to conduct surveillance away from the workplace as a "last resort" can be reasonable.[181] As well, in a workplace where security concerns are paramount, such as a nuclear plant, even the collection and disclosure of current spousal information does not run afoul of *PIPEDA*.[182]

Alberta's Commissioner has determined in one case that video surveillance was not done in contravention of *PIPA* so long as it was directed at loss prevention, safety and security rather than at managing employee performance.[183]

Initially, privacy statutes were limited to *recorded* personal information,[184] but the more recent ones, *PIPEDA* and *PIPA*, contain a more expansive approach to personal information that proceeds from the perspective of the identifiable individual rather than restricting the definition of personal information to that which is recorded.[185] The distinction means, therefore, that the newer statutes, in contrast to the older ones, apply to unrecorded video surveillance.[186] However, simply attempting to record employees' conversations by installing in a staff room a recording device that failed to record anything has recently been held not to be a violation of *PIPEDA*.[187]

The decisions on surveillance are legion.[188]

---

180 *PIPEDA* Case Summary #265 "Video cameras in the workplace," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp>. A similar conclusion was reached in *PIPEDA* Case Summary #279 "Surveillance of employees at work," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp>.

181 *PIPEDA* Case Summary #269 "Employer hires private investigator to conduct video surveillance on employee," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2004/cf-dc_040423_e.asp>, consistent with *PIPEDA*, *supra* note 5, s. 7(1)(b).

182 *Re Ontario Power Generation Inc. and Society of Energy Professionals* (2004), 128 L.A.C. (4th) 265 (Ont.).

183 *Report of an Investigation into Collection and Use of Personal Employee Information Without Consent, R.J. Hoffman Holdings Ltd.* (13 May 2005), Investigation Report P2005-IR-004, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/P2005_IR_004May13.pdf>.

184 *FOIPPA*, *supra* note 4, s. 1(n), *Privacy Act*, *supra* note 5, s. 3.

185 *PIPEDA*, *supra* note 5, s. 2; *PIPA*, *supra* note 5, s. 1(k).

186 See "Opinion by retired Supreme Court Justice Hon. Gérard V. La Forest, C.C., Q.C." (19 November 2002), online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/media/nr-c/opinion_021122_lf_3.asp> addressed to George Radwanski, Privacy Commissioner of Canada and the discussion about the first *PIPEDA* decision (Summary #1), 15 June 2001, in the text at note 8.

187 *Morgan v. Alta Flights (Charters)* (2005), 138 A.C.W.S. (3d) 409, 2005 FC 421 (T.D.).

188 See Barbara McIsaac *et al.*, *The Law of Privacy in Canada* (Scarborough: Thomson Carswell, 2000) at 2.5.3.4.

B. DRUG AND ALCOHOL TESTING

Generally, mandatory drug and alcohol testing is not justified even in sensitive safety positions in the absence of a real suspicion supported by demonstrable evidence that the employee has a problem which is affecting performance. Monitoring of behaviour away from the workplace, even if the after-effects of drugs and alcohol remain discernable in the employee at work, is a serious intrusion into the employee's privacy rights and places a high burden on the employer to justify it.[189]

Oddly, to date, neither the federal nor the Alberta Commissioner appears to have issued a decision concerning alcohol and drug testing, except for one investigation report dismissing a complaint against the City of Calgary Fire Department for the intrusiveness of the personal information required of job applicants on its Personal History Statement form, relating to driving, alcohol use, drug use, credit and criminal activity, "detected or undetected."[190] No actual testing for substance abuse was involved. Nevertheless, Alberta's Commissioner has commented:

> With respect to drug and alcohol testing, the case law to date has established that in the absence of an express statutory or contractual authority, there must, once again, be a compelling employer interest in administering drug and alcohol tests (i.e. objective evidence of alcohol and drug impairment in the workplace), a significant connection between the test results sought and the employee's work duties (i.e. a safety concern), and a no less intrusive alternative, before workplace drug and alcohol testing policies have been condoned by the Courts and arbitrators. Even where there is a statutory or contractual authority to conduct testing, such testing must be performed in a reasonable and non-discriminatory fashion, and the employer must demonstrate a reasonable likelihood that the testing will be effective in reducing or eliminating impairment in the workplace.[191]

As in the case of video surveillance, a number of factors must be balanced in determining whether the employer's drug and alcohol testing policy or practices are reasonable. For example, where the operations are safety-sensitive, the employer need not prove the

---

189 *Ibid.* at 2.5.5; Allan Hope, "Drug/Alcohol Testing and Workplace Privacy An Arbitrator's Perspective" in Whitaker 2001-2002, *supra* note 1 at 85-99; William Armstrong, "Drug/Alcohol Testing and Workplace Privacy A Management Perspective," in Whitaker 2001-2002, *ibid.* at 101; Jeffrey Andrew, "Drug/Alcohol Testing and Workplace Privacy A Union Perspective," in Whitaker 2001-2002, *ibid.* at 119; Eugene Oscapella, "Drug Testing and Privacy 'Are You Now, Or Have You Ever Been, A Member of the Communist Party?' McCarthyism, Early 1950's. 'Are You Now, or Have You Ever Been, A User of Illicit Drugs?' Chemical McCarthyism, 1990s" in William Kaplan *et al.*, eds., *Canadian Labour Law Journal*, vol. 2 (Toronto: Butterworths-Lancaster House, 1994) 325; B. Hovius *et al.*, "Employee Drug Testing and the Charter" in Kaplan, *ibid.*, 345; Joan McEwen, "Addressing Chemical Dependency-Related Issues in the Workplace: A Proposed Model for Workplace Health and Productivity" in Kaplan, *ibid.*, 421; Susan Charlton, "Trade Union Concerns about Substance Abuse in the Workplace" in Kaplan, *ibid.*, 439; Catherine Wedge, "Limitations on Alcohol and Drug Testing in Collective Bargaining Relationships" in Kaplan, *ibid.*, 461; Mel F. Belich & Michael Shewchuk, "Drug Testing in the Transportation Sector: An Employer Perspective" in Kaplan, *ibid.*, 516.

190 *Report on Investigation Regarding Collection, Use and Disclosure of Personal Information, City of Calgary - Calgary Fire Department* (10 June 2003), Investigation Report F2002-IR-012 ACF7C3E, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/ACF7C3E>.

191 Presentation by Frank Work on 17 May 2004, at Nymity's Employee Privacy Conference, reported in PrivaViews, online: Nymity <www.nymity.com/privaviews/2004/Work.asp> at 5.

existence of a drug and alcohol problem before introducing testing.[192] However, a much more employee-oriented perspective can be derived from human rights cases which treat drug and alcohol dependencies as disabilities requiring accommodation from the employer to the point of undue hardship.[193]

If the employer and union have agreed on a program of drug and alcohol testing, and in particular if provision is made for it in the collective agreement, then the balancing of rights has already been achieved by the parties. In such a case, there is no breach of privacy for the employer to insist on testing an employee who the employer has reason to believe is a substance abuser but not yet a safety risk. If the employee refuses, there is just cause for termination.[194] Breaching a drug and alcohol policy again after earlier discipline for similar infractions can certainly justify termination.[195] However, termination of current employees in non-safety-sensitive positions for refusing to be tested under a new drug and alcohol policy is improper and the matter was sent back to an Alberta Human Rights panel for further consideration.[196]

After a lengthy review of the jurisprudence in this area and applying it to the employer's proposed drug and alcohol policy, the arbitrator in *Esso Petroleum Canada v. Communications, Energy & Paperworkers' Union, Local 614*[197] held that it was proper to conduct mandatory testing of employees in safety-sensitive positions, so long as it was conducted by the employees' own physicians and the results as reported to the employer were limited to fitness or unfitness for the job.

It was also pointed out in *Esso Petroleum* that "the testing technology overshoots the mark and is of questionable validity."[198] The reliability of the results of drug and alcohol testing is of concern, not only because of the difficulty of proper interpretation and application of the results to the issues at hand, but also because of reports that there is a significant risk of cheating, by means of fake specimen samples, *etc.*

C. ELECTRONIC MONITORING

Finally, we return to records. *PIPEDA*, as its name implies, addresses electronic documents in ss. 33-47, but as alternatives to paper records and traditional transactions

---

192 *Re Weyerhaeuser Company Ltd. and Industrial, Wood and Allied Workers of Canada* (2004), 127 L.A.C. (4th) 73 (B.C.).

193 See *e.g. Milazzo v. Autocar Connaisseur Inc.*, [2003] C.H.R.D. No. 24, 2003 CHRT 37 (Canadian Human Rights Tribunal) (QL) (summary termination of bus driver with perceived drug disability after positive drug test rather than attempting accommodation measures impermissible). See also *North American Construction Group Inc. v. Alberta Human Rights and Citizenship Commission* (2003), 362 A.R. 29, 2003 ABQB 755 (Commission ordered to proceed with complaint alleging discrimination in connection with a failed pre-employment drug test).

194 *Re Fluor Constructors Canada Ltd. and International Brotherhood of Electrical Worders, Local 424 (Chorny)* (2001), 100 L.A.C. (4th) 391 (Alta.).

195 *Imperial Oil Ltd. v. Communications, Energy and Paperworkers Union of Canada, Local 777 (Parsons Grievance)*, [2001] A.G.A.A. No. 102 (Alta.) (QL).

196 *Alberta (Human Rights and Citizenship Commission) v. Elizabeth Metis Settlement* (2005), 367 A.R. 142, 2005 ABCA 173, rev'g (2003), 336 A.R. 343, 2003 ABQB 342.

197 [1994] B.C.C.A.A.A. No. 244 at paras. 244-48, 273 (B.C.) (QL) [*Esso Petroleum*].

198 *Ibid.* at para. 273.

accomplished by means of paper records. In the information society, it is necessary to make provision for electronic information exchanges and record-keeping which, unlike paper, are instantaneous, ephemeral and hard to erase. Electronic records, websites, chat rooms and electronic monitoring challenge the privacy of personal information in whole new ways. Instead of exchanging information with persons, we interact with websites which gather or leave information, in the form of "cookies" and personal information tracking, which is often overinclusive and intrusive.[199]

Employer e-mail monitoring of employees is reported to be widespread.[200] Employers consider computer equipment used by employees and what is stored on it to be their property to be used only for business purposes, while employees regard their codes and the messages they send to be their own "mail" and subject to a reasonable expectation of total privacy. For these reasons, employers need to promulgate clear policies to their employees on Internet use and e-mail monitoring, although a "common sense" principle should assist employers who catch their employees sending or receiving inappropriate e-mail or visiting inappropriate websites.

When the employer is the service provider of the e-mail system, the employee's expectation of privacy in the system is lower than if the employee is accessing the Internet to send e-mails.[201]

Keystroke logging systems enable the employer to monitor not just an employee's e-mail use, but everything the employee does on the computer. Alberta's Commissioner has held that while not all of the information disclosed through keystroke logging is necessarily personal information, even the errors in a transcription or the speed of performance of the task can be personal information because they give the monitoring employer information about an identifiable person. This degree of information-gathering was not warranted in the circumstances because the employer could not demonstrate that the employee used his computer more than once for personal matters or that there were performance issues. There were less intrusive ways of addressing performance concerns, particularly since the employee was not told of the keystroke logging and there was no policy on accepted uses of the public body's computers.[202]

Employee consent or proper notification is, therefore, required in most cases for monitoring e-mail or computer use. Notification can occur through the use of comprehensive computer and Internet use policies, with consent being obtained when the employee is given

---

199 See "Protecting Your Privacy on the Internet," online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/fs-fi102_05_d_13_e.asp>; "Faxing and Emailing Personal Information" (February 2005), online: Information and Privacy Commissioner of British Columbia <www.oipc.bc.ca/sector_private/public_info/index.htm>.

200 McIsaac, *supra* note 188 at 2.5.4. See also Janis Sarra, "Employee Use of E-Mail and the Internet An Arbitrator's Perspective" in Whitaker 2001-2002, *supra* note 1 at 11; Russell Albert & Karen McBean, "Employee Use of E-Mail and the Internet A Management Perspective" in Whitaker 2001-2002, *ibid.* at 33; Lorne Richmond, "Employee Use of E-Mail and the Internet An Union Perspective"in Whitaker 2001-2002, *ibid.* at 45.

201 *R. v. Weir* (1998), 213 A.R. 285, 1998 ABQB 56, aff'd (2001), 281 A.R. 333, 2001 ABCA 181.

202 *Parkland Regional Library* (24 June 2005) Order F2005-003, online: Office of the Information and Privacy Commissioner of Alberta <www.oipc.ab.ca/ims/client/upload/F2005-003.pdf>.

access to the computer. The purpose of monitoring the employee's computer use must be explained to the employee and any information collected can only be used for that purpose, unless consent for some other purpose is obtained. As with video surveillance, if the employer has reasonable and probable grounds to suspect that the employee has breached an agreement or law, then it may be possible to monitor e-mail and computer use without consent.[203]

Employers who put in place systems for monitoring electronic communications must keep in mind s. 184 of the *Criminal Code*[204] which makes it an indictable offence to willfully intercept without consent a private communication by electro-magnetic, acoustic, mechanical or other device.

VI. CONCLUSION

The privacy statutes are stark indicators of our "rights" culture, where individuals expect to be able to protect themselves against intrusive actions from others and to be given the legal tools to do so. They remind us that the collective activities of the workplace no longer dominate our culture. The production and manufacturing of "real" goods is yielding ground to information technology as the work product of our age. In such an environment, privacy concerns are likely to consume an ever larger proportion of workplace energy and focus.

---

[203] See David Corry & Laura Mensch, "Employee Privacy: Impact on the Workplace of the New Federal *Personal Information Protection and Electronic Documents Act*" (presented at the 20th Annual University of Calgary Labour Arbitration and Policy Conference, June 2002).

[204] *Criminal Code*, R.S.C. 1985, c. C-46.