Employment Privacy

Discussion Paper & Guidelines

DISCUSSION DRAFT ONLY (JUNE 2004)

1.0 Introduction

Privacy issues arising from the employment relationship are becoming both increasingly complex and pressing. Employees spend a large percentage of their waking hours at work, and it is recognized that they have a significant dignity interest in maintaining a right of privacy in the workplace. At the same time, employers have a strong business interest in monitoring employee activity in order to address a variety of concerns, ranging from detecting and deterring employee theft to ensuring a safe and harassment-free workplace. Technological advances will continue to provide employers with a wide range of monitoring options, many of which can operate without the employees' knowledge. Moreover, it is well accepted that the employment relationship is such that willing and informed employee consent to working conditions such as employee monitoring cannot reasonably be implied solely from the decision to maintain an employment relationship.

In the past, employee privacy concerns have been addressed in the decisions of labour arbitrators, in human rights decisions and, to a lesser extent, through the common law. In an effort to define the content of an employee's right or claim to privacy, decision-makers have looked to a variety of sources, including the *Canadian Charter of Rights and Freedoms*, provincial legislation regarding privacy and human rights, and specific employment agreements While each case turns on its specific facts and the particular legislative framework involved, a number of principles have been quite consistently recognized throughout Canada. In addition, various bodies around the world that are charged with examining privacy issues have attempted to outline principles which should be recognized in addressing employment privacy concerns.

The purpose of this paper is to discuss privacy in the employment context and how British Columbia's *Personal Information Protection Act* ("PIPA") affects the collection, use, disclosure and protection of personal information in the workplace. It is also intended to provide context for proposed guidelines for three representative workplace privacy issues—the collection of information in the pre-employment context; the electronic monitoring of employees (including video, telephone and voicemail surveillance, as well as computer and email monitoring); and the collection of personal information through drug and alcohol testing.

2.0 Privacy in the Workplace

PIPA specifically addresses privacy in the context of the employment relationship and provides a framework for balancing the privacy "rights" of employees and the business "interests" of employers. In undertaking this balancing exercise, the purpose clause contained in s. 2 of PIPA refers to the "right" of the individual (employee) against the "interest" of the organization (employer), as follows:

> **2.** The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

In some respects, the specific requirements set out in PIPA reflect a statutory codification and acceptance of principles which have emerged from the arbitral and other jurisprudence. However, most of the requirements in PIPA are expressed in general terms and therefore will require interpretation. To promote rational and consistent application of PIPA, and to encourage PIPA compliance, the Office of the Information and Privacy Commissioner for British Columbia ("OIPC") believes it is desirable to set out the guiding principles that will govern PIPA's interpretation. These principles, and their interpretation and application, may be informed by development of the law in the arbitral and human rights context and by experience in other jurisdictions regarding employment privacy. These will only be relevant, of course, to the extent that they are consistent with the language and structure of PIPA itself.

The requirement of reasonableness permeates the various PIPA provisions that may affect employee privacy and employer rights. In considering the question of reasonableness, it is appropriate to balance the dignity interest of employees with the business interests of employers. Employers have a right to direct the workforce and thus have a legitimate interest in monitoring employee productivity. Further, employers exercise ownership rights over materials, equipment, and intellectual property and have a legitimate interest in ensuring there is no security threat to these interests. Employers provide benefit plans and are entitled to ensure they are not abused. Finally, employers may be vicariously liable for the acts of their employees and thus have an interest in preventing and detecting employee wrongdoing that may result in employer liability to other employees or to third parties. The reasonableness of any infringement of employees' privacy rights by an employer will depend on the nature and extent of the intrusion and the significance of the interest which the employer seeks to protect.

At the same time, it must be remembered that employees and employers share many interests in the operation of the workplace. Both employers and employees have an interest in maintaining a healthy, harassment-free work environment so that the employer's interest in monitoring employee behaviour in this regard should not be seen as necessarily being in strict opposition to employee interests. Similarly, both employers and employees have a strong interest in ensuring that workers are treated with respect, thereby promoting their productivity.

3.0 PIPA and the Employment Context

PIPA regulates the collection, use and disclosure of personal information by organizations other than government bodies. Most private sector employers in British Columbia, including not-for-profit organizations, are now governed by PIPA.

PIPA applies to all personal information collected by organizations, whether that information relates to customers, employees or other persons. This paper is only concerned with the rights and obligations of organizations as employers in relation to the privacy rights of their employees.

3.1 Definitions

The definition of "employee" in PIPA includes apprentices, volunteers, and co-op students.

Because there is a wide range of information which employers collect about their employees, it is important to consider the various definitions relating to personal information set out in PIPA. This is because the nature of the information, and the purposes for which it is collected, will determine what obligations are associated with its collection, use and disclosure.

PIPA places statutory constraints on the collection, use and disclosure of "personal information". It defines "personal information" as "information about an identifiable individual". PIPA treats collection, use and disclosure of "personal information" differently from how it treats "contact information", "work product information" and "employee personal information". The focus of this document is on how PIPA treats "employee personal information", but the following outlines how PIPA addresses "contact information" and "work product information".

Contact information is information that enables an individual at a place of business to be contacted. It includes information such as one's business address, business telephone number and position, name or title. PIPA does not regulate collection, use and disclosure of contact information.

The definition of "personal information" also excludes "work product information", which is defined in PIPA as follows:

> Information prepared or collected by an individual or group of individuals as apart of the individual's or groups' responsibilities or activities related to the individual's or group's employment or business but does not include personal information about an individual who did not prepare or collect the information.

Because work product information is excluded from PIPA's definition of personal information, PIPA does not regulate the collection, use and disclosure of work product information.

Personal information includes "employee personal information", which is, in some ways, subject to different treatment under PIPA than personal information generally. PIPA defines "employee personal information" as:

> Personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment.

Where an employer collects, uses or discloses personal information of its employees that does not fit within the definition of "employee personal information", PIPA's general requirements will apply to collection, use and disclosure.

3.2 Application of PIPA

With certain exceptions set out in PIPA, PIPA requires that an individual consent to the collection, use or disclosure of personal information about that person. In order to obtain consent, the organization must disclose to the individual the purposes for which the information is being collected. Consent will be implied if the information is voluntarily provided and the purpose for the collection, use of disclosure would be obvious to a reasonable person. Consent is deemed to be given for the collection, use or disclosure of information for the purpose of enrolment or coverage in an insurance, pension, benefit or similar plan, for the beneficiary or insured under the plan. Consent can also be deemed to have been given if the individual does not decline to consent after having been given reasonable opportunity to do so and after having been provided with notice that an organization intends to collect, use or disclose that individual's personal information. The latter category, of deemed consent, also requires that the collection, use or disclosure be reasonable given the sensitivity of the information. Section 9 of PIPA sets out the consequences of a withdrawal of consent.

Employee personal information can be collected, used or disclosed *without* consent if the collection, use or disclosure is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual *and* the employer has given the employee prior notice that such collection, use or disclosure is to take place. That notice must include disclosure of the purposes for the collection, use or disclosure of the employee personal information.

Both employee personal information and personal information more generally can be collected, used or disclosed without consent or notice in certain circumstances set out in PIPA. The exception to the consent requirement that is most likely to be relevant in the employment context is when obtaining consent would compromise the availability or accuracy of information and its collection, use or disclosure which is reasonable for an "investigation" or a "proceeding". PIPA defines "investigation" to *include* an investigation related to a breach of an agreement, which would include an employment agreement (individual or collective).

Personal information of employees may also be disclosed without their consent in relation to matters such as the purchase, sale, merger or amalgamation of an organization. However, the organization receiving the personal information must notify employees, and others whose personal information has been disclosed, that the business transaction has taken place and that their personal information was disclosed as part of the transaction.

PIPA gives individuals whose personal information is collected, used or disclosed by an organization the right of access to their own personal information, and to request that it be corrected if it is inaccurate. PIPA also imposes a duty on an organization to implement reasonable safeguards for personal information in its custody or its control. These rights and obligations apply equally to employee personal information and other personal information of employees.

Another way in which PIPA affects the employment relationship relates to the protection given to employees who disclose a contravention of PIPA or who act to prevent a contravention of PIPA (so-called "whistleblowing"). An organization is prohibited from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee or denying the employee a benefit on the basis that the employee has, acting in good faith and on the basis of reasonable belief, disclosed a contravention of PIPA or acted to avoid a contravention of PIPA. Contravention of this provision by the organization or its representatives constitutes an offence.

In addition to fines for breaches of PIPA, an individual has a cause of action in the courts against an organization for compensation for damages suffered by the individual as a result of the breach. The cause of action arises under s. 57 of PIPA only after the Commissioner has made an order confirming that the organization has breached the Act or after the organization has been successfully prosecuted for the breach of PIPA. An employee could, therefore, have a cause of action against his or her employer resulting from the employer's breach of PIPA.

4.0 PIPA and Employment Contracts

PIPA explicitly sets out the obligations of employers with respect to the collection, use, disclosure and care of the personal information of employees. These obligations are the same, whether an employee works under a collective agreement, under an individual contract of employment, or as a volunteer. To the extent that an employment agreement is silent on the obligations of an employer with respect to the collection, use, disclosure and care of employees' personal information, PIPA creates new obligations for the employer. For those unionized employees whose privacy rights were recognized in some fashion by arbitrators, PIPA may lead to these rights being better defined and more consistently enforced.

The relationship between PIPA's requirements and those obligations that are explicitly set out in employment agreements is complex. The terms of the employment

agreement may be relevant in determining the content of obligations under PIPA. For example, in determining whether the collection or use of personal information is reasonable for the purposes of maintaining an employment relationship, a term of the employment agreement that relates to such information will be a relevant consideration.

The parties to an employment agreement can likely agree that a given procedure or activity will discharge a party's obligations under PIPA as long as this represents a genuine attempt to fulfill PIPA's requirements. However, a provision should not be aimed at depriving the OIPC of the ability to determine reasonableness under PIPA. For example, it may be permissible for the parties to agree, as a matter of contract, that adequate notification of monitoring activities will be assumed where the employer publishes notice of such monitoring practices in a specific way. However, it is likely not valid for the parties to agree that any kind of collection of information for the purposes of preventing employee theft will be deemed to be reasonable.

While PIPA is silent on the whether parties can contract out of its provisions, the obligations imposed by PIPA are statutory requirements and very likely cannot be waived by consent. Human rights legislation is read into all employment agreements, so if there is a conflict between the terms of a collective agreement and human rights legislation, the legislation prevails. Similarly, because the legislature has provided that PIPA will prevail over the terms of any inconsistent legislation unless the other legislation expressly provides otherwise, privacy rights as reflected in PIPA should take precedence over other statutory entitlements and enforcement of collective agreements. This would mean that any terms of an employment contract—including a collective agreement—which attempt to contract out of PIPA's provisions would be void and unenforceable, both as a matter of contract law and with respect to the enforcement of PIPA itself.

While the parties ought not to be able to contract out of their obligations under PIPA, they may agree to take on additional obligations through the employment agreement. For example, it is probably not valid for an employment agreement to state that the employer is free to undertake the collection of personal information of the employees without notification or consent. However, the parties might agree that the employer can only collect such information with consent, notwithstanding that under PIPA some of that information gathering would only require notification.

Employment Privacy Guidelines

These guidelines, published by the Office of the Information and Privacy Commissioner for British Columbia ("OIPC"), are intended to promote rational and consistent interpretation and application of British Columbia's *Personal Information Protection Act* ("PIPA") in relation to the privacy of employees and employers' interests. It is the responsibility of individual employers to ensure, in each case, that they comply with PIPA's requirements and with the requirements of all other applicable laws and agreements.

1.0 Pre-Employment Collection of Information

These guidelines apply to all collection of information by employers from prospective employees in the pre-employment context.

1. Requests for personal information in the pre-employment context should clearly identify whether the information is sought for hiring purposes or some other purpose. If it is sought for some other purpose, or if it is not reasonably required for employment purposes, the request for information should clearly state that the individual is free to refuse to disclose the information, and that this refusal will not affect the hiring process. Best practice is to contact only references provided by the applicant.

2. Information relating to the prohibited grounds in the *Human Rights Code*, namely, an applicant's race, colour, ancestry, place of origin, political belief, religion, marital status, family status, physical or mental disability, sex, sexual orientation or age, or the fact that the individual has been convicted of a criminal or summary conviction offence that is unrelated to the employment or to the intended employment of that person, is not reasonably required for employment purposes, unless it relates to a *bona fide* occupational requirement.

3. Pre-employment medical testing will only be reasonably required for employment purposes where the employer can demonstrate that the particular medical condition being tested for is related to a bona fide occupational requirement.

4. Other types of testing must be demonstrated to represent accurate methods of measuring attributes that are required for the job concerned. Any form of testing which reveals highly personal information will only be considered reasonable only if the employer demonstrates a high degree of correlation between the test results and the ability to fulfill the basic duties of the job, or a pressing employer interest which outweighs the invasion of the employees' privacy.

5. In disclosing the purpose of gathering information through testing, prospective employees should be told the attributes that a test purports to be assessing.

6. Personal information disclosed in pre-employment situations must not be used or disclosed for any other purpose, unless that purpose is stated at the time of collection and the use or disclosure is reasonable for that other purpose.

7. If personal information collected is used in the hiring decision, PIPA requires that it must be retained for at least one year so that each individual affected by the hiring decision has a reasonable opportunity to access it. Employers must make reasonable security arrangements to protect the confidentiality of information collected at the pre-employment stage.

8. Employees and unsuccessful applicants must be given an opportunity to examine and correct their personal information collected at the pre-employment stage. If this includes test results, employees should be given their results in a format which they can understand, as well as sufficient information about the test to ascertain its accuracy. All individuals have a right under PIPA to have access to, and to request correction of, their personal information held by an organization.

2.0 Electronic Monitoring with Notification

These guidelines apply to non-surreptitious electronic monitoring of employees. This would include video surveillance in the workplace, email and internet use monitoring, and telephone and voice mail monitoring. It does not include monitoring which only collects work product information as defined in PIPA. All monitoring must meet both the notification and reasonableness requirements set out in PIPA.

2.1 Reasonableness Requirement

1. The employer must have a substantial and compelling concern which would justify monitoring and must give notice that the monitoring is being done for that specific purpose.

2. The more serious the intrusion into the employee's privacy, the more substantial the employer's concern will need to be. For example, the short-term use of video surveillance for training purposes may have very little impact on privacy and may be justified by concerns about increasing productivity. Similarly, monitoring the volume of email may have little impact on employee privacy and may be easily justified. By contrast, continuous video monitoring, or the monitoring of private email content, would require a much more significant employer concern in order to be justified.

3. Monitoring should be designed to be as least intrusive of the employee's privacy as possible. Video cameras should be rotating and should not be directed at areas of the workplace that have a high degree of privacy associated with them,

such as change rooms or lounge areas. Email and computer monitoring should gather as little information as possible while still addressing the legitimate concerns of the employer.

4. Employers should be prepared to demonstrate that monitoring is necessary in order to achieve their purposes, or at least that it will be substantially more effective than other methods of doing so.

5. Information gathered by way of monitoring can only be put to use for those purposes for which notification was given at the time the monitoring was undertaken.

6. Information gathered by way of monitoring must be protected by reasonable security arrangements.

7. If the information is to be used to make a decision about the employee, or if the information is likely to be disclosed to another organization, the employer must make reasonable efforts ensure that the information is accurate and complete.

8. If the information is used to make a decision about the individual, PIPA requires that it must be kept for at least one year. Otherwise, the employer must destroy the information, or remove the means by which it can be identified with an individual, as soon as the purpose for which it was collected is not longer being served and retention is not required.

2.2 Notification Requirement

1. Notification should state the purposes for collecting the information. The *Criminal Code*[1] allows interception of a private communication if it is essential to identify, isolate or prevent harm to a computer system. This amendment underscores the importance of employers creating and communicating clear policy regarding employee use of employer computers about what is acceptable and not acceptable use of the employer's computers.

2. Notification should state the circumstances under which the information may be used or disclosed.

3. Notification should state the type of employee activity which is being monitored. For example, if a mobile telephone is being used to monitor the location of employees, it is not sufficient to state that telephone usage will be monitored.

4. Notification must state the type of monitoring system employed and locations at which monitoring devices are operative.

---

[1] s. 184 as amended by Bill C-14, 2004 which received Royal Assent on April 22, 2004.

5. Notification must state the degree of monitoring which is occurring. For example, it is not sufficient to state that email use will be monitored; the employer must state whether it intends to monitor the actual content of the emails, or just the subject line, or just volume of email. As noted above, employers should create and communicate clear policy regarding employee use of employer computers about what is acceptable and not acceptable use of the employer's computers.

6. Notification of monitoring should be brought to the attention of employees on a regular basis.

7. Notification should explicitly state the policies or requirements with which the employer is monitoring compliance, or at least clearly refer to those policies and where they can be found.

8. Notification of monitoring should occur each time there is a change in:

   (a) the employer's monitoring policy, or
   (b) in any of the policies regarding behaviour which may be monitored.

   As an example of (b), if the employer changes its policy regarding acceptable Internet use, it must provide notice of monitoring along with the notice of change in the Internet policy.

3.0 Electronic Monitoring Without Notification or Consent

These guidelines apply to any covert monitoring of employees by employers. This includes any monitoring without notification, whether it takes place in the workplace or elsewhere. PIPA requires that such monitoring take place only in the specific circumstances set out in PIPA, and that it also meet the test of reasonableness.

3.1 Exceptions to the General Rule requiring Notice or Consent

1. Information can only be gathered covertly, that, is, without consent or notification, in the circumstances set out in s. 12(1) of PIPA.

2. If s. 12(1)(c) is relied on for authority to obtain information by covert monitoring, the employer must be prepared to demonstrate both:

   (a) that it is reasonable to believe that a breach of an employment agreement has taken place, and

   (b) that there is an ongoing investigation into a specific allegation.

3. The employer must be prepared to demonstrate that collection with consent or

notification would compromise the availability or the accuracy of the personal information.

3.2 Reasonableness Requirement

1. The employer must be prepared to demonstrate that the collection was reasonable for the purposes of the investigation. Covert monitoring is highly intrusive of privacy interests and thus requires a high level of justification to be reasonable.

2. The employer must have a substantial and compelling concern which would justify monitoring. A concern for safety, or serious, demonstrated security concerns may justify monitoring.

3. Any monitoring should be designed to be as least intrusive of the employee's privacy as possible. Monitoring should not occur in situation where an employee has a high expectation of privacy.

4. Monitoring should only gather the minimum amount of information necessary for the employer's purposes.

5. Employers should be prepared to demonstrate that there was no reasonable alternative to monitoring.

6. Information gathered by way of monitoring must be protected by reasonable security arrangements. In addition, if the information is to be used to make a decision about the employee, or if the information is likely to be disclosed to another organization, the employer must make reasonable efforts ensure that the information is accurate and complete. If the information is used to make a decision about the individual, PIPA requires that it must be kept for at least one year. Otherwise, the employer must destroy the information, or remove the means by which it can be identified with an individual, as soon as the purpose for which it was collected is not longer being served and retention is not required.

4.0 Drug and Alcohol Testing

These guidelines apply to the taking of breath, urine, or blood samples for the purpose of determining drug or alcohol use. Such testing can only be used for employment purposes if it is reasonable to do so. What is reasonable may be different for an alcohol test, which is capable of determining impairment at a particular time, than for a drug test, which can only show the use of drugs at some previous time.

1. Pre-employment drug or alcohol testing is not reasonable.

2. Drug or alcohol testing in non-safety-sensitive positions is not reasonable.

3. Random drug testing of employees is not reasonable because it cannot determine whether an employee is impaired by drug use at a particular time.

4. In order to require random alcohol testing of employees, an employer must demonstrate that there is a problem with alcohol use in the workplace that cannot be adequately addressed by other methods such as education, increased supervision of the employees, and increased training of supervisors.

5. In order to require drug or alcohol testing of an individual employee, an employer must demonstrate:

   (a) that there are reasonable grounds, based on an informed and probable suspicion, to believe that the individual employee has been impaired in the workplace. Such reasonable grounds may be established by, for example, the discovery of drug paraphernalia in the workplace or a report from a co-worker. Reasonable grounds may also be established where an employee voluntarily discloses a substance abuse problem, or where an employee is returning to work after recovery from a substance addiction; or

   (b) that the employee has been involved in a work place accident or near accident and that there are reasonable grounds to believe that impairment may have been a factor in the accident or near accident.

6. An employer may only require drug or alcohol testing in accordance with the law of another jurisdiction if such testing is necessary in order to allow the employee to fulfill their duties in that jurisdiction.

7. An employer must make reasonable efforts to ensure that information obtained from a drug or alcohol test is accurate. This means that they must use reliable testing methods and must provide employees who test positive a subsequent opportunity to take the test, in order to protect against the danger of false positives.

8. Drug or alcohol test results that are used to make a decision affecting an employee must be retained for at least one year. PIPA also requires that the test results must be provided to the employee at his or her request, and the employee must have an opportunity to challenge the accuracy of the test result. Reasonable security arrangements must be made to protect the confidentiality of the test results.

9. Information obtained from a drug or alcohol test cannot be used for a purpose other than the purpose for which it was collected. Nor can an employer use a bodily sample that was provided for a reasonable employment purpose to obtain

other information. For example, an employer must not conduct a pregnancy test using a blood sample that was provided for the purpose of determining whether an employee had been impaired in the workplace.