Evans, Philp LLP
Barristers and Solicitors

Breakfast Series:

# Workplace Privacy

## Where Does It Begin?
## Where Does It End?

February 1, 2007

# *Workplace Privacy*

Presenters:

Brent Foreman, LLB
Philip Bender, LLB

Evans, Philp LLP
Barristers & Solicitors
1 King St. W., 16th Fl.
(905) 525-1200
www.evansphilp.com

# *Workplace Privacy : What Are The Limits?*

"How much intrusion into employee privacy is justifiable? The answer largely depends upon who is being asked this difficult question, but there is a general consensus that privacy is not an absolute right, particularly in the employment context…."

66 Sask L. Rev. 383

# *Workplace Privacy : The Common Law*

- **Is There A Common Law Right To Privacy?**

  "…a common law right of privacy is not universally accepted…[the] courts have protected privacy rights by expanding the scope…of established torts [such as] trespass, nuisance, negligence, defamation and injurious falsehood, misappropriation of personality, breach of confidence, and fiduciary duty …."

  66 Sask. L. Rev. 383

# *Workplace Privacy: If Not The Common Law…*

- **Other Sources of Privacy Rights:**
  - Federal Legislation
  - Provincial Legislation
  - Employment Contracts
  - Collective Agreements

# *Workplace Privacy: Federal Legislation*

- **Personal Information Protection and Electronic Documents Act [PIPEDA]**

  "I should caution you at this point about a frequent misunderstanding. While the application of [PIPEDA] will expand in 2004 to commercial activities that normally fall under provincial jurisdiction, it won't extend to employment in those activities."

  George Radwanski
  (former Federal Privacy Commissioner), June 16,2003

# *Workplace Privacy: Provincial Legislation*

- **FIPPA, MFIPPA & PHIPA**

  **Freedom of Information and Protection of Privacy Act [FIPPA]**

  - applies to provincial ministries and agencies boards, most commissions, community colleges, district health councils

# *Workplace Privacy: Provincial Legislation*

- **FIPPA, MFIPPA & PHIPA, cont'd**

  **Municipal Freedom of Information and Protection of Privacy Act [MFIPPA]**

  - applies to municipalities, local boards, agencies and commissions and may include information held by a city clerk, a school board, board of health, public utility or police commission

# *Workplace Privacy: Provincial Legislation*

- **FIPPA, MFIPPA & PHIPA, cont'd**

  **Personal Health Information Protection Act [PHIPA]**

  - applies to:

    (a) the collection of personal health information by a health information custodian;

    (b) the use or disclosure of personal health information by,

    (i) a health information custodian, or

    (ii) a person who is not a health information custodian and to whom a health information custodian disclosed the information

# *Workplace Privacy: Medical Information*

- "Personal Health Information" – any information that could be used to identify an individual that relates to:
  - the physical or mental health of the individual;
  - the provision of health care to the individual, including the identification of the health care provider;
  - payments or eligibility for health care in respect of the individual;
  - the donation by the individual of any body part or bodily substance; or
  - the individual's provincial health number.

# *Workplace Privacy: Medical Information*

- Who are Health Information Custodians?
  - Regulated health professionals
  - Drugless practitioners and social workers
  - Hospitals, nursing homes, pharmacies, ambulance services, laboratories, community or mental health centres
  - Ministry of Health and Long-Term Care
  - “Agents” who are authorized to access, use or control personal health information for the purposes of the organization.

## *Workplace Privacy: Medical Information*

- Organizations such as employers, insurance companies or schools that request or have personal health information of an individual, are not HIC's
- These non-custodians become bound to the "use" and "disclosure" rules when personal health information is received from a HIC

## *Workplace Privacy: Medical Information*

- Employers who are also HIC's must differentiate between the two roles and maintain proper practices and procedures for information obtained in these respective roles
- Company doctors or occupational health nurses (HIC's) may have competing obligations

# *Workplace Privacy: Medical Information*

- Employer may only use or disclose an employee's personal health information for the authorized purpose for which consent was given
- HIC's must ensure they obtain "knowledgeable" consent from individual before disclosing personal health information

# *Workplace Privacy: Medical Information*

- Consent:
  - Must be the consent of the individual
  - Must be “knowledgeable”
  - Must relate to the information
  - Must not be obtained through deception or coercion
- Consent must be express if disclosure is to a non-HIC

# *Workplace Privacy: Medical Information*

- "Knowledgeable" consent:
  - The purposes for the use, collection or disclosure of the information
  - That the individual may give or withhold their consent
- Consent can be withdrawn at any time, but cannot be withdrawn retroactively

# *Workplace Privacy: Medical Information*

- Information an employer is entitled to:
  - Sufficient information to permit it to satisfy itself that a particular absence was for a *bona fide* sickness or disability
    - General nature of the injury/illness
    - Functional abilities/limitations
    - Prognosis
    - Expected date of return

# *Workplace Privacy: Medical Information*

- Information an employer is not entitled to:
  - Specific diagnosis of the injury or illness
  - Nature of the medical treatment received
- Scope of information depends on the circumstances
  - the stage of the inquiry
  - who has access to the information
  - whether any term in collective agreement provides for the disclosure of medical information

# *Workplace Privacy: Medical Information*

- What should employers do?
  1. Ensure that any HIC in their employ is aware of duties and responsibilities under *PHIPA*
  2. Maintain controlled location for the storage of employees' personal health information
  3. Maintain separate human resources and health information files
  4. Obtain proper consent, including purpose and use of the information requested

## *Workplace Privacy: Surveillance*

- *Charter* does not directly apply to private entities
- Values enshrined in *Charter* must inform common law principles
- Does not guarantee an absolute right of privacy to employees

# *Workplace Privacy: Surveillance*

- Must be a reasonable expectation of privacy in any given set of circumstances
- Differing levels of privacy which an individual can expect:
  - Relatively low expectation of privacy when in public
  - Higher expectation of privacy when in ones home

# *Workplace Privacy: Surveillance*

- Two part test for admissibility of surveillance evidence:
  1. Was it reasonable in the circumstances?
  2. Was the surveillance itself conducted reasonably?

     Were there other, less intrusive alternatives open to the employer by which it could obtain the evidence it was looking for?

## *Workplace Privacy: Surveillance*

- Surreptitious surveillance in the workplace generally requires greater justification
- Surveillance implicates an entire group of employees as being potential wrongdoers
- Surveillance of a group of employees for disciplinary purposes is the highest form of intrusion

# *Workplace Privacy: Surveillance*

- Stringent test for surreptitious surveillance in the workplace:
  - Demonstrate that there is a substantial problem and a strong probability that surveillance will assist in solving the problem
  - Show that employer has exhausted all available alternatives
  - Ensure that surveillance is conducted in a systematic and non-discriminatory manner

    (*St. Mary's Hospital* decision)

# *Workplace Privacy: Surveillance*

- Non-surreptitious surveillance has a lower threshold:

  "…the test is whether surveillance is a reasonable exercise of management rights in all circumstances of the case."

  (*Unisource Canada* decision)

# *Workplace Privacy: Surveillance*

- Cameras used as a deterrence to theft is a valid use of managements rights
- However, cameras trained on employee production areas are inconsistent with goal of deterrence (*Unisource Canada* decision)
- Distinction has been recognized between security cameras and ‘process’ cameras (*Pope & Talbot* decision)

## *Workplace Privacy: Surveillance*

- Decision to proceed with surveillance should be based on more than mere suspicion
- Employer should be cautious and properly investigate dubious claims before commencing surveillance:
  - Information from coworkers should be carefully reviewed and corroborated, where possible
  - Employers should request further medical information and offer light duties

# *Workplace Privacy: Workplace Computers*

- **Some Considerations Relevant To Workplace Computers:**

Employment Relations Considerations Include:

- to what extent does an employee have a "*reasonable expectation of privacy*" ?
- to what extent does the employer have a legitimate interest in monitoring computer usage or accessing computers?

# *Workplace Privacy: Workplace Computers*

- **Some Considerations Relevant To Workplace Computers, cont'd**

Property Law Considerations Include:

- employer's right to protect, and employee's obligation to respect, the employer's confidential *proprietary* information
- employer's right to control the computers and associated software that it owns

# *Workplace Privacy: A Common Sense Approach*

"Privacy is in its infancy as a public policy issue,…we all have a lot of work ahead of us in adjusting to the new realities and expectations of members of the public and our customers. However, ….good privacy is, to a large extent, really just good common sense. The principles and values that underlie privacy are simple to understand, easy to accept, and relatively straightforward to implement."

Tom Mitchinson, Assistant Ontario Privacy Commissioner, May 16, 2003

# *Workplace Privacy: Some Suggestions*

- **Use the legislation as a guide:**

  Employers not covered by ***PIPEDA, FIPPA*** or ***MFIPPA*** may wish to use ***PIPEDA*** as a guide for how to manage the collection, storage, release and destruction of private information relating to employees

# *Workplace Privacy: Some Suggestions*

- **Incorporate *PIPEDA* principles in your policies:**

  ***PIPEDA*** principles that may serve as a useful guide to employers include:

  1. **ACCOUNTABILITY**
  2. **IDENTIFYING PURPOSES**
  3. **CONSENT**
  4. **LIMITING COLLECTION**
  5. **LIMITING USE, DISCLOSURE AND RETENTION**
  6. **ACCURACY**
  7. **SAFEGUARDS**
  8. **OPENNESS**
  9. **INDIVIDUAL ACCESS**

# *Workplace Privacy: Some Suggestions*

- **Be aware of the competing rights and interests:**

  When dealing with the accommodation of disabilities in the workplace, keep in mind the interplay between:

  1. Privacy rights; and,
  2. The *Human Rights Code* obligation of the employer, the employee and the union (where applicable) to exchange meaningful information relevant to the search for an appropriate accommodation

# *Workplace Privacy: Some Suggestions*

- **Be rational and persistent**

  Do not assume that a refusal of an employee and/or the union (where applicable) to authorize the release of certain medical information is justifiable or reasoned– i.e. care, patience and persistence often are required to obtain the necessary information to which the employer is entitled

# *Workplace Privacy: Some Suggestions*

- **Implement a computer use policy**

  **Develop** and **distribute** among staff a clear policy regarding the use of company computers and software, the ownership of information and the right to access the contents of an employee's computer

# Evans, Philp LLP Breakfast Series Continues

Next Presentation: March 27, 2007

## The Duty to Accommodate: Obligations of Employers, Employees and Unions