

# **PRIVACY IN PRACTICE: TOP 10 WORKPLACE Q&As**

**ANDREA YORK  
PARTNER**

416.863.5263  
andrea.york@blakes.com

---

*Blakes*

PRIVACY IN PRACTICE:  
TOP 10 WORKPLACE Q&As

TABLE OF CONTENTS

---

|            |   |           |
|------------|---|-----------|
| <b>1.</b>  | <b>WHICH LAW APPLIES?.....</b>  | <b>1</b>  |
|            | (a) PIPEDA.....   | 1         |
|            | (b) PHIPA.....  | 3         |
|            | (c) Arbitral jurisprudence.....   | 3         |
|            | (d) Common law.....   | 4         |
| <b>2.</b>  | <b>WHAT KIND OF EMPLOYEE CONSENT IS NEEDED? .....</b>   | <b>5</b>  |
| <b>3.</b>  | <b>WHAT KINDS OF BACKGROUND CHECKS ARE PERMITTED?<br/>WHEN? .....</b>                           | <b>6</b>  |
| <b>4.</b>  | <b>CAN AN EMPLOYER DISCLOSE EMPLOYEE INFORMATION TO<br/>OTHERS WITHOUT CONSENT? .....</b>       | <b>9</b>  |
|            | (a) Workplace Violence.....   | 9         |
|            | (b) Sale of business .....  | 11        |
|            | (c) References .....  | 12        |
|            | (d) Police and governmental agency requests .....   | 13        |
| <b>5.</b>  | <b>ARE EMPLOYERS PERMITTED TO MONITOR EMPLOYEE EMAIL OR<br/>INTERNET ACTIVITIES?.....</b>       | <b>14</b> |
| <b>6.</b>  | <b>CAN EMPLOYERS INSTALL VIDEO CAMERAS AT WORK?.....</b>  | <b>15</b> |
| <b>7.</b>  | <b>CAN EMPLOYERS INSTALL BIOMETRIC SECURITY SYSTEMS?.....</b>                                   | <b>18</b> |
| <b>8.</b>  | <b>DO EMPLOYERS HAVE TO GIVE EMPLOYEES ACCESS TO THEIR<br/>PERSONNEL FILES?.....</b>            | <b>21</b> |
| <b>9.</b>  | <b>CAN EMPLOYERS TRANSFER EMPLOYEE PERSONAL<br/>INFORMATION TO AFFILIATES IN THE U.S.?.....</b> | <b>21</b> |
| <b>10.</b> | <b>WHAT KINDS OF POLICIES SHOULD EMPLOYERS IMPLEMENT? .....</b>                                 | <b>22</b> |

---

*Blakes*

## PRIVACY IN PRACTICE: TOP 10 WORKPLACE Q&As

---

Andrea York

In Ontario, most employers are generally required to balance their desire to collect, use and disclose employee personal information with an employee's desire to protect his or her own privacy. The purpose of this paper is to briefly review some of the questions that are commonly asked by Ontario employers, describe some of the best practices in response to those questions and to provide insight into the latest developments in privacy law.

### 1. **WHICH LAW APPLIES?**

Perhaps the question, "Which law applies?", is not a question that arises frequently when fielding questions from employers. However, knowing the underlying law is essential to determining how to respond to the various frequently asked questions that do arise. As such, it is an appropriate place to begin this discussion.

#### **(a) PIPEDA**

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") governs both federally and provincially regulated employers to varying degrees.<sup>1</sup> While organizations such as banks, telecommunication companies, shipping and international transportation companies and other federal undertakings are regulated federally and statutes such as the *Canada Labour Code* are applicable to them, the vast majority of

---

<sup>1</sup> R.S.C. 2000, c. 5.

---



employers are provincially regulated.<sup>2</sup> In Ontario, provincially regulated employers are subject to the *Employment Standards Act, 2000*.<sup>3</sup>

PIPEDA governs a federally regulated employer's collection, use and disclosure of employee personal information in all contexts. For provincially regulated employers, PIPEDA only governs an employer's handling of employee personal information in the context of a commercial activity. It does not apply to a provincially regulated employer's ordinary collection, use and disclosure of employee personal information in the course of establishing, maintaining or terminating the employment relationship in Ontario. Accordingly, PIPEDA has a much narrower application to provincially regulated employers.

It bears noting that recently proposed amendments to PIPEDA would give federally regulated employers more freedom to handle employee personal information in the context of the employment relationship. Consent to collect, use or disclose employee personal information would not be required in the context of establishing, managing or terminating the employment relationship, provided that the employer has notified the individual that the personal information will be or may be collected, used or disclosed for these purposes. This amendment would bring PIPEDA more in line with the privacy legislation applicable to provincially regulated employers in British Columbia and Alberta.

---

<sup>2</sup> R.S.C. 1985, c. L-2.

<sup>3</sup> R.S.O. 2000, c. 41.

**(b) PHIPA**

There is no comprehensive privacy legislation that governs provincially regulated employers in Ontario. However, questions regarding an employer's obligations under the Ontario *Personal Health Information Protection Act, 2004* ("PHIPA") sometimes do arise.<sup>4</sup> The main objective of PHIPA is to establish rules for the collection, use and disclosure of personal health information and to protect the confidentiality of that information. In general terms, PHIPA applies to the collection of personal health information by a health information custodian ("HIC"), such as a hospital, and the use or disclosure of personal health information (or a health number) by a HIC.

PHIPA will apply to the collections, uses and disclosures of health information by and to an Ontario employer only if the employer is a HIC (for example, where employers have medical facilities onsite), or if the employer receives health information from a HIC. Not surprisingly, if an employer receives health information from a HIC, it should only use that information for the purposes for which it was disclosed to the employer, or otherwise only with the consent of the employee.

**(c) Arbitral jurisprudence**

Even if neither PIPEDA nor PHIPA directly applies to a particular collection, use or disclosure of personal information by an employer, if the workplace is unionized, the employer may be subject to some significant limitations on its ability to collect, use and disclose personal information. Arbitrators in labour relations cases have been rather vigilant in ensuring that unionized workers have a right to privacy in employment. This

---

<sup>4</sup> O. Reg. 329/04.

has been particularly apparent where employers have attempted to implement video surveillance or biometric security systems, as discussed in more detail below.

**(d) Common law**

While unionized workers enjoy protection from invasion of privacy through the arbitration process, non-unionized workers have less tangible privacy rights in the workplace. There are two emerging causes of action that employees may claim in cases where they are asserting privacy rights.

The first is a tort claim for invasion of privacy. While Canadian courts have often been reluctant to establish an independent tort of invasion of privacy, in at least one decision of the Ontario Superior Court of Justice, the court held that: “the time has come to recognize invasion of privacy as a tort in its own right”.<sup>5</sup>

The second claim is in contract. In *Colwell v. Cornerstone Properties Inc.* (“*Colwell*”), an employer installed a secret video camera above a manager’s desk. When the employee discovered the camera and the employer provided her with an implausible explanation for the installation of the camera, she claimed constructive dismissal.<sup>6</sup> In this case, rather than focusing on whether the employer had committed a tort, the court focused on the contract of employment and found that the breach of privacy caused by the camera constituted a fundamental breach of that contract.

As a result, going forward, we are more likely to see perceived invasions of privacy arising in constructive dismissal claims. However, since damages awarded for tort claims are not taxable, we might also see creative plaintiff’s counsel include a claim

---

<sup>5</sup> *Somwar v. McDonald’s Restaurants of Canada Ltd.*, [2006] O.J. No. 64 at para. 31.

<sup>6</sup> [2008] O.J. No. 5092 (S.C.J.) (QL) [*Colwell*].

related to the tort of invasion of privacy to the list of claims for damages in wrongful or constructive dismissal litigation.

## 2. **WHAT KIND OF EMPLOYEE CONSENT IS NEEDED?**

The answer to this question depends on the context. One of the key requirements of Canadian privacy legislation is the obligation to obtain informed consent, usually before or at the time of collection, use or disclosure of personal information. Employers often question whether they need the consent of their employees in certain contexts, and if so, what they need to do in order to obtain such consent.

Although the statutory requirements differ from jurisdiction to jurisdiction in Canada, the general rule is that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. The individual must have knowledge of the purposes for which their personal information is being collected, used and disclosed. The information provided must also be in a format that the individual can understand.

Consent may be express or implied. Generally, consent may be implied when it can be shown that the purpose of the collection, use or disclosure of the information was reasonably obvious to the individual, where a reasonable person would expect the information to be collected, used or disclosed for those purposes, and where it is reasonable to assume that the individual consented. The more sensitive the information being collected, the more likely it is that express consent should be obtained. Detailed employee notices and policies for activities such as employee internet monitoring and video surveillance monitoring will go a long way in assisting employers in demonstrating that there was implied consent to collect employee personal information.

---

The logo for the law firm Blakes, featuring the name "Blakes" in a stylized, cursive script font.

**3. WHAT KINDS OF BACKGROUND CHECKS ARE PERMITTED? WHEN?**

Background checks conducted by employers can range anywhere from checking a job applicant's references and education history, to obtaining criminal, motor vehicle and credit history reports. Background checks on job applicants are generally permissible in Canada, but there are some limitations with respect to the scope of such checks and what an employer may do upon receipt of negative results.

It has generally been the case that, with proper consent, an employer was permitted to conduct background checks as a condition of employment. Due to the fact that the questions asked in order to conduct a background check and the results obtained sometimes touch on grounds that are protected by human rights legislation, the Ontario Human Rights Commission and others have taken the position that employers should make conditional offers of employment prior to conducting a background check. However, until recently, there were otherwise few other restrictions with respect to such pre-employment screening.

A recent investigation report of the Alberta Information and Privacy Commissioner (*Mark's Work Warehouse Ltd.*) under Alberta's *Personal Information Protection Act* suggests that pre-employment screening practices will come under more scrutiny where privacy legislation applies.<sup>7</sup> Many employers have long believed that a good credit rating is an indicator that an individual is less likely to commit theft or fraud. In the *Mark's Work Warehouse Ltd.* case, the Alberta Privacy Commissioner found that conducting pre-employment credit checks on employment applicants is not reasonably required to assess an applicant's ability to perform his or her job duties or to assess

---

<sup>7</sup> See Investigation Report P2010-IR-001 (16 February, 2010) and R.S.A. 2003, c. P-6.5 (respectively).

whether he or she might have a tendency toward committing theft or fraud. As such, the employer agreed to cease performing credit checks as part of its hiring process.

While the *Mark's Work Warehouse* decision may have little impact on provincially regulated employers in Ontario, to the extent that the same reason can be applied under PIPEDA, it is likely to come as a surprise to many financial institutions which are governed by PIPEDA and where credit checks are commonly conducted.

In addition to credit checks, it has become more difficult for employers to conduct criminal record checks on prospective or existing employees. The RCMP has implemented a new and sometimes time-consuming process for obtaining criminal records in Canada. In some cases, applicants will be required to attend at a police station and provide fingerprints in order to obtain a certificate certifying whether he or she has a criminal record.

In addition, a recent case brings into question the practice of conducting mid-employment criminal records checks. In *Ottawa (City) v. Ottawa Professional Firefighters Assn.*, the Divisional Court dismissed an employer's application for judicial review and upheld the decision of an arbitrator finding that the employer was not permitted to conduct wholesale criminal background checks on a regular basis on all existing employees.<sup>8</sup> The arbitrator found that there was a "significant distinction between the point of initial hire and the normal course of business in an ongoing employment relationship". While the arbitrator indicated that establishing a policy requiring a given employee to consent to a criminal background check where there was reasonable grounds to justify it would be acceptable, the Divisional Court appeared not

---

<sup>8</sup> [2009] O.J. 2914 (S.C.J.) (QL).

to be persuaded that this would be permissible pursuant to the *Municipal Freedom of Information and Protection of Privacy Act*.<sup>9</sup> The court questioned whether the statute would ever permit the privacy rights of employees to be taken away from them through a unilateral policy established by their employer. Accordingly, depending on the legislation applicable to the employment relationship, there may be significant restrictions on an employer's ability to conduct criminal background checks on existing employees.

In light of these decisions, it would appear that courts, commissioners and arbitrators may be more willing to place restrictions on an employer's ability to conduct background checks involving the potential collection of sensitive personal information where the background check is not reasonably related to the employee's ability to perform his or her job duties. As a best practice, employers should generally consider the following when conducting background checks:

Consider why the background check is needed, whether it will provide the employer with the information desired and what actions will be taken when there is a negative result.

Obtain employees' express consent to collect, use and disclose the information. Advise employees or applicants of the purpose(s) for which the information is being collected and limit the type and amount of information collected to that purpose(s).

If a criminal record check is required, due to the time involved in obtaining the record under the new RCMP rules, consider advising job applicants to obtain their own criminal records.

---

<sup>9</sup> R.S.O. 1990, c. M.56.

---

*Blakes*

If a third party service provider is retained for the purpose of conducting background checks, ensure that the employee is aware that a service provider will be collecting information on behalf of the employer. Ensure, through contract, that the service provider will not use or disclose the information collected for its own purposes.

Ensure that, once the personal information concerning employees is collected, it is safeguarded from unintentional or inappropriate disclosures. Limit the personnel who have access to background check information. Ensure that any third party service provider handles the information in a manner that complies with privacy legislation.

Retain any personal information only as long as necessary to fulfil the purposes for which it was collected. Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.

**4. CAN AN EMPLOYER DISCLOSE EMPLOYEE INFORMATION TO OTHERS WITHOUT CONSENT?**

Most employers are careful to ensure that sensitive personal information collected about employees is kept confidential unless they have the consent of the employee to disclose that information. However, there may be circumstances where the employer is not required to obtain consent.

**(a) Workplace Violence**

Recent amendments to the *Occupational Health and Safety Act* (“OHSA”), commonly known as Bill 168, require employers to disclose information related to the risk of workplace violence from existing employees or others to protect the health and

---

The logo for Blakes, featuring the word "Blakes" in a stylized, cursive script font.

safety of workers.<sup>10</sup> In particular, section 32.05(3) imposes a duty on employers and supervisors to provide information, including personal information, to a worker related to a risk of workplace violence from a person with a history of violent behaviour if: (a) the worker can be expected to encounter that person in the course of his or her work; and (b) the risk of workplace violence is likely to expose the worker to physical injury. However, section 32.05(4), states that no employer or supervisor shall disclose more personal information than is reasonably necessary to protect the worker from physical injury.

This amendment leads to some interesting privacy questions. Employers may consider asking employees or potential employees whether they have a history of workplace violence. Employers will be required to assess whether any existing employees, suppliers or other individuals who have access to the workplace, pose a threat to any of their workers. If the assessment reveals that the individual does pose a threat to any of the workers, employers and supervisors are then required to disclose that information to workers. While the goal is to protect the health and safety of the workers, the employer will want to avoid liability for common law privacy or defamation claims which could be commenced by the individual to whom the information pertains. Although the OHSA applies to provincially regulated employers, if the information is about a supplier or other individual with whom the employer has a commercial relationship, PIPEDA might also apply to the disclosure such that there is also a risk of a privacy complaint. There might also be the potential for human rights complaints if the risk of violence arises as a result of a disability. It remains to be seen how employers will balance these risks.

---

<sup>10</sup> R.S.O. 1990, c. O.1.

**(b) Sale of business**

In the context of a sale of the employer's business, it is not uncommon for the potential purchaser to request significant and sometimes sensitive personal information about the seller's employees as part of the due diligence process. Due to the fact that PIPEDA applies to commercial activities of both federally and provincially regulated employers, and the fact that the sale of a business might fall within the ambit of a commercial activity, there has been a concern about whether an employer is required to obtain the consent of the employee to disclose their personal information in this context. Since the preliminary due diligence process is often confidential and sometimes subject to strict securities law requirements, obtaining employee consent is not practical or possible in most cases. Recently proposed amendments to PIPEDA appear to address this concern.

The proposed amendment to PIPEDA would include a new exception to the consent requirement permitting disclosures and uses of information in connection with a "prospective business transaction". In the newly proposed section 7.1, parties to a prospective business transaction would be permitted to use and disclose personal information without the knowledge or consent of the individual if they have entered into an agreement that requires the recipient to use and disclose the information solely for purposes related to the transaction, to protect that information with appropriate safeguards and, if the transaction does not proceed, to return or destroy the information within a reasonable period of time. It would also be a condition that any personal information disclosed during the process be necessary to determine whether to proceed with the transaction and complete the transaction. Once the transaction is completed, the proposed subsection 7.1(2) would permit the parties to the transaction to use and disclose the personal information without consent, provided they have entered into an agreement that requires them only to use the information for the purposes for which it was originally collected, to protect that information and to give effect any withdrawal of

---

*Blakes*

consent. This provision that permits the use and disclosure of personal information for business transactions does not apply to business transactions where the primary purpose or result is the purchase, sale or other acquisition of personal information.

**(c) References**

Reference requests are another common situation where an employer may be asked to disclose information about an existing or former employee. Many employers have policies or practices that provide that only dates of hire and the employee's position will be disclosed in response to such requests. However, there are certain advantages to providing accurate and positive references, particularly following a dismissal without cause where mitigation income earned by the employee can reduce the employer's post-termination financial obligations to the employee. On the other hand, the disclosure of negative information about former employees may hinder the employee's chances of obtaining alternative employment.

Where PIPEDA applies to an Ontario employer, the employer will want to ensure that it has consent before discussing the employee with a potential employer. If no privacy legislation applies, employers may be free to respond to reference requests with or without the consent of the employee. However, given the risk of being exposed to common law claims related to privacy or defamation, employers will want to proceed cautiously, particularly if the comments regarding the employee would be negative. With respect to any claim of defamation, an employer might be in a position to rely on the defence that the comments were the truth or that they were protected by qualified privilege, but most employers will want to avoid the potential for litigation. Accordingly, even provincially regulated employers will want to ensure that there is consent to respond to reference requests and might consider declining such requests if there is little to say that is positive.

---

The logo for the law firm Blakes, featuring the name in a stylized, cursive script font.

**(d) Police and governmental agency requests**

Employers are also sometimes asked by police departments for an employee file to assist in a criminal investigation. This practice may have implications for an employee's protected privacy interests. In *R. v. V.I.*, the Ontario Superior Court of Justice found that the police had unlawfully collected information about an employee who was the subject of a criminal investigation because the police had failed to obtain a search warrant before requesting files from the employer.<sup>11</sup> The court found that the police should have applied for a warrant and that, in failing to do so, the police infringed upon the employee's rights under Section 8 of the *Canadian Charter of Rights and Freedoms*.<sup>12</sup> The court held that:

Employment records typically contain a wide spectrum of information concerning employees... For example, they may contain financial information, performance appraisals, discipline records, as well as highly private information of a medical or psychiatric nature. In a related context, s. 278.1 of the Criminal Code, which addresses the issue of the production third-party records, defines a private record as "any form of record that contains personal information for which there is a reasonable expectation of privacy". Employment records are specifically enumerated as falling within this definition.<sup>13</sup>

Since it remains open for an employee to make a claim or complaint against an employer for improperly disclosing his or her personal information to the police without consent, employers ought to proceed with some caution before responding to police requests.

---

<sup>11</sup> [2008] O.J. No. 2856 [V.I.].

<sup>12</sup> Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

<sup>13</sup> V.I., *supra* note 11 at para. 7.

Other common requests for employee personal information may come from governmental agencies such as Service Canada when an employee applies for Employment Insurance following the termination of the employment relationship. In those circumstances, employers would do well to ask the governmental agency to identify their lawful authority to obtain the information.

5. **ARE EMPLOYERS PERMITTED TO MONITOR EMPLOYEE EMAIL OR INTERNET ACTIVITIES?**

In general terms, the answer to this question is “yes”. However, the extent to which an employer may conduct such monitoring and the actions that an employer may take when it discovers inappropriate use of email or internet activity may be limited. The Federal Privacy Commissioner prefers that employers engage in targeted monitoring when wrongdoing is suspected, rather than engage in wholesale monitoring of all online activities. Nonetheless, courts, privacy commissioners and arbitrators have generally accepted that reasonable monitoring is permissible, provided that employees are advised that monitoring occurs and that there is no reasonable expectation of privacy when using company email and internet systems.<sup>14</sup>

Before implementing any monitoring, employers should implement a policy that clearly notifies employees that they have no reasonable expectation of privacy with regard to their e-mail and internet usage and that regular monitoring will be conducted. If the employer intends to monitor employees’ social media activities outside of work, the employees should be advised of that fact. Employees must be advised of the purposes for which such information is being collected. In addition, employees ought to be advised as to what activities are not permissible and the consequences for breaching

---

<sup>14</sup> Office of the Privacy Commissioner of Canada, Findings under the *Privacy Act*, “Manager is justified in tapping into employee’s e-mail account” (2006-2007).

the policy. With such a policy in place, employers may reasonably take the position that they have consent to the collection of any personal information collected through email and internet monitoring.

It is important to note, however, that not all breaches of such a policy will constitute cause for termination. As with all breaches of policy, the policy must be consistently applied and any discipline imposed must be proportional.

#### **6. CAN EMPLOYERS INSTALL VIDEO CAMERAS AT WORK?**

The answer to this question is a qualified “yes”, depending on where and why the cameras are installed and what activities are being videotaped. It is trite to say that video surveillance can be highly privacy intrusive. The Federal Office of the Privacy Commissioner will rely on the following four-point test in surveillance cases: 1) Is the use of video surveillance cameras (or other technology) demonstrably necessary to meet the specific need? 2) Is the surveillance likely to be effective in meeting these needs? 3) Is the loss of privacy proportional to the benefit gained? 4) Is there a less privacy-invasive way of achieving the same end?

In PIPEDA Case Summary #2009-001, an employer that installed numerous video cameras in a bus depot claimed there was implied consent for the use of video surveillance in the bus depot by virtue of the clearly visible surveillance cameras, the fact that video surveillance has been used in major transportation terminals in Canada for several years, and the fact that there were signs at the entrance of the depot alerting the public to the existence of video surveillance. In responding to the organization’s claim of implied consent, the Assistant Commissioner found:

Implied consent of employees for the use of their personal information collected by video surveillance is assumed to have been obtained when the personal information being collected is not sensitive and the express purposes of the video surveillance have been explained so that the

---

*Blakes*

employees would reasonably expect that their information be used for those purposes...

While consent could be considered implied in this case, and signs in the terminal provide limited information about the video cameras, there had been at the time of the complaint no detailed explanation of the cameras' purposes provided to the employees. For this reason, Principle 4.3.2 was contravened.<sup>15</sup>

With respect to the issue of surreptitious video surveillance of employees, the *Colwell* case referred to above created a stir in the employment law bar when the judge found that installing a secret video camera above a manager's desk constituted constructive dismissal. In that case, the employer's position was that the camera was installed to detect thefts thought to have been perpetrated by maintenance staff after hours. The manager, herself, was not advised of the installation of the camera, it was the only camera in the area, and it is not clear how any thief would use the manager's desk to "review the loot". Accordingly, Justice Little found the employer's explanation to be implausible and went on to find:

A secret camera being installed in a trusted manager's office without her knowledge, although perhaps acceptable employer conduct in itself, coupled with a totally implausible explanation, renders the actions unacceptable.

Mrs. Colwell, at the time of trial, was not even aware of two of the three alleged prior thefts. No cash was retained in her office nor had any of the alleged thefts taken place from her office. Mr. Krauel's explanation that he thought the thieves might move into her office to "review the loot" is preposterous and merely compounded the issue.

---

<sup>15</sup> Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2009-001, "Bus terminal video surveillance is challenged by company employee" (findings issued 19 February 2009).

---

*Blakes*

Why was Mrs. Colwell not told of the existence of the camera if she was not meant to be the one under surveillance? Why was the camera not activated only when the maintenance staff was there after hours? What was the real reason for installing the camera?

The cost to human dignity caused by such surveillance, coupled with the unbelievable explanation subsequently provided, left Mrs. Colwell in a position of being unable to rely upon the honesty and trustworthiness of her immediate supervisor, and amounted to more than merely “bad faith” and “unfair dealing”.<sup>16</sup>

PIPEDA Case Summary #2007-379 also indicates that surreptitious monitoring will be closely scrutinized.<sup>17</sup> In this case, employees complained that the state of the men’s washroom was a mess. The employer began monitoring employees coming and going from the washroom after receiving the complaint. Notwithstanding that the employer limited the monitoring to a period of three days, ceased monitoring after ascertaining the culprit, had undertaken the monitoring to address a health and safety problem and was able to catch the perpetrator through such monitoring, the Assistant Privacy Commissioner found that the employees’ complaint was well-founded. The employer could have used less privacy-intrusive means of identifying the employee who was making a mess of the men’s washroom.

At a minimum, an employer ought to include a description of its video monitoring practices in a policy and post signs indicating that video surveillance or monitoring is conducted. Employees must be informed of all purposes for which such monitoring is

---

<sup>16</sup> *Colwell*, *supra* note 6 at paras. 30-33.

<sup>17</sup> Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2007-379, “Condition of washrooms prompts management to monitor facilities” (findings issued 4 April 2007).

conducted. It is also a good practice for employers to consider and potentially exhaust other means of obtaining the information in a less privacy-invasive manner first and limit the collection of personal information (e.g. if after-hours security is a risk, turn the cameras on only after hours). In the end, employers must bear in mind that a decision maker will determine whether a reasonable person would consider it appropriate to use the cameras to manage the problem at issue.

## 7. **CAN EMPLOYERS INSTALL BIOMETRIC SECURITY SYSTEMS?**

Biometric technology uses unique physical attributes of an individual, such as a fingerprint or voice, to identify that individual. In most cases, the technology involves scanning the physical attribute, reducing it to digital form and storing it on a system so that it can be used for comparison purposes. Each time the individual wishes to gain access to the place or system protected by the biometric technology, the physical attribute is again scanned and the new scan is compared against the stored sample. If the two match within a preset threshold, the individual is granted access. Among other things, biometrics can now be used in time clocks to verify employee work hours, for security purposes in door locks, and in computer and telephone systems. However, there are several cases where employees have challenged the implementation of biometric systems on privacy grounds.

One of the better known biometrics in the workplace cases remains the Federal Court of Appeal (“FCA”) decision in *Wansink v. Telus Communications Inc.*, (“*Wansink*”).<sup>18</sup> In this case, Telus sought to introduce a voice recognition system for security purposes. The employees claimed that Telus breached a number of the privacy principles set out in PIPEDA by implementing the new system. The employees

---

<sup>18</sup> [2007] F.C.J. No. 122 (F.C.C.A.) (QL).

argued that they did not consent to this system, and that Telus was wrongfully threatening to impose discipline on all employees who did not comply with the system requirements and provide voiceprints. The FCA found that the Trial Division judge had correctly analyzed the privacy interests of the employees by considering whether the reasonable person would find Telus' use of technology to be reasonable at the time the impugned collection of information occurred. The Court held that:

It is also trite law that privacy rights under PIPEDA are not absolute. Their amplitude is to be determined through a balancing process whereby, in a case such as this one, the private interests of the employees and the business interest of the employer are to be considered in order to define the permissible limits of intrusion in an employee's privacy.<sup>19</sup>

The FCA referred to the factors to be considered in determining whether the use of technology was reasonable at paragraph 16:

1. the degree of sensitivity associated with the information collected;
2. the security measures implemented to protect the information;
3. the *bona fide* business interest of the employer, established through evidence, that is the purpose of the collection or use of personal information;
4. the effectiveness of the privacy-invading act in pursuing the employer's *bona fide* business interest;
5. the reasonableness of the method used as compared to other comparable methods (considering effectiveness, cost and level of security); and

---

<sup>19</sup> *Ibid.* at para. 10.

6. the proportionality of the loss of privacy weighed against the costs and operational benefits of the infringing conduct in light of security mechanisms in place.

Although the FCA adopted the Privacy Commissioner's findings that the encroachment on privacy rights was minimal and that the use of the technology was reasonable, it found that Telus was required to obtain employee consent. However, the FCA found that Telus had sought employee consent before collecting the voice information and was satisfied that the consent received was not vitiated by any meaningful threat of discipline or actual discipline. The FCA agreed with the Trial Division that the implementation of the voice recognition system did not violate PIPEDA because the decision to use the system was reasonable.

In the more recent arbitral decision of Agropur, Division Natrel v. Teamsters, Local Union 647 (Milk and Bread Drivers, Dairy Employees, Caterers and Allied Employees) (Time Management System Grievance), the union grieved the employer's decision to use a time-management system that used fingerprint scans to confirm employee identity.<sup>20</sup> The system scanned less than half of the employee's fingertip. The new system had been introduced without prior notice or consultation but the biometric element had not yet been implemented. The employer conceded that privacy interests were engaged but argued that the invasion was not significant and that the system was necessary as there had been incidents of buddy-punching at the plant. That said, the employer conceded that buddy punching was not a serious or widespread problem. The employer presented evidence that the information was secure: the

---

<sup>20</sup> [2008] O.L.A.A. No. 694 (QL).

---

*Blakes*

information stored would be extremely difficult to access and, if accessed, would be of no use as it was stored in a jumbled format.

The arbitrator found that although the employer's reasons for implementing the system were not pressing or crucial, they were legitimate. In addition, the arbitrator held that the proposed system included rigorous security protections for the information collected in the scans, and that, because of the way the information was stored, such information would be useless to other parties, including law enforcement authorities. The intrusion of privacy was permissible because it was "extremely small, almost negligible" and the employer's business reason was legitimate.

**8. DO EMPLOYERS HAVE TO GIVE EMPLOYEES ACCESS TO THEIR PERSONNEL FILES?**

The answer to this question is straightforward. Pursuant to PIPEDA, federally regulated employers must allow employees access to their personal information following receipt of a written request. Exceptions to this rule include where granting access would likely reveal personal information of a third party and the personal information cannot be severed or where the information is protected by solicitor-client privilege. However, in the absence of one of the stated exceptions, access must be granted.

In contrast, provincially regulated employers in Ontario have more freedom to refuse an access request. In the absence of a court order, summons or contract requiring disclosure, an employer is not legally obliged to allow employees access to their own personal information.

**9. CAN EMPLOYERS TRANSFER EMPLOYEE PERSONAL INFORMATION TO AFFILIATES IN THE U.S.?**

Many Canadian employers have head offices in the U.S. In an effort to reduce costs, a number of those employers have consolidated human resources systems

---

*Blakes*

between Canada and the U.S. Transferring information to the U.S. may give rise to concerns that the U.S. anti-terrorism and other authorities will have access to that information under the U.S. *Patriot Act*, which permits the U.S. authorities to require that companies disclose personal information to the authorities without notifying the individual to whom the information pertains. In light of these concerns, the best practice from an employment and privacy law perspective is for the employer to notify the employees that their information will be transferred to the U.S. The notice should also advise the employees of the purposes for which the information will be transferred and the uses that the affiliate will make of the personal information. Finally, the notice should also contain a statement that, once the information is transferred outside of Canada, it will then be subject to the laws of the jurisdiction in which it is retained.

#### **10. WHAT KINDS OF POLICIES SHOULD EMPLOYERS IMPLEMENT?**

Policies notify employees what the employer is doing with employee personal information and why. Employers can go a long way in fending off privacy-related complaints from employees with proper policies in place or by providing other forms of notices to employees about how their personal information will be handled. Privacy policies are required under PIPEDA and under other provincial privacy legislation. Such policies may not only advise employees how the company handles personal information, but can also explain the consequences to the employees for failing to safeguard personal information that they receive during the course of their work. Further, in addition to the usual email and internet policies, social media policies are also becoming more commonplace. In a 2009 speech given at the IAPP Canadian Privacy Summit entitled, "Social Networking and the New Rules of the Road", Jennifer Stoddart, the Privacy Commissioner of Canada, urged employers to develop policies

---

The logo for the law firm Blakes, featuring the name "Blakes" in a stylized, cursive script font.

specifying the appropriate use of social networking sites at work and what monitoring the employer will be conducting on social media sites.<sup>21</sup> If an employer intends to implement video surveillance of any employees, a video surveillance policy is also advisable.

## **CONCLUSION**

In the decade since PIPEDA was introduced, there have been some significant changes to technology allowing us to collect, use and disclose information, and law-makers have been attempting to keep pace with those changes. Whether or not there is privacy legislation that applies to a particular collection, use or disclosure of personal information, existing privacy legislation provides important principles that all employers should consider following when handling employee personal information. In doing so, employers are more likely to avoid costly litigation or grievances as the common law and arbitral jurisprudence continues to develop.

---

<sup>21</sup> Jennifer Stoddart, "Social Networking and the New Rules of the Road" (IAPP Canadian Privacy Summit, Toronto, Ontario, 30 April 2009), online: Office of the Privacy Commissioner of Canada <[http://www.priv.gc.ca/speech/2009/sp-d\\_090430\\_e.cfm](http://www.priv.gc.ca/speech/2009/sp-d_090430_e.cfm)>.