Privacy Quiz

QUESTION

Can an employee voluntarily give up any expectations of privacy in the workplace by consenting or agreeing through a waiver procedure to effect that purpose?

ANSWER

Some employers may take the position that loss of privacy is a condition of employment. These employers may implement a waiver procedure to accomplish this.

Whether such a procedure is clear, informed, voluntary consent is dubious at best. Courts in all jurisdiction view waivers with skepticism. A waiver must meet the rigorous legal test of being clear, informed, voluntary and free of threats and intimidation.

PREAMBLE

Employers and employees are often subject to privacy laws. The *Privacy Act*, for example, applies to employee information in federal government institutions. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to employee information in federal works, undertakings, and businesses. Several provinces have privacy legislation applying to employee information. In addition, employers often make a commitment in collective agreements to observe privacy practices.

But whether or not privacy is protected by law or contract, respecting privacy in the workplace makes good business sense.

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.

Employers can balance their “need to know” with their employees’ right to privacy, if they ensure that they collect, use, and disclose personal information about their employees for appropriate purposes only.

WHY IS IT RIGHT

RULES RESPECTING EMPLOYEES’ PRIVACY

An employer’s need for information should be balanced with an employee’s right to privacy. For almost all personal information – including pay and benefit records, formal and informal personnel files, video or audio tapes, and records of web-browsing, electronic mail, and keystrokes – **the following basic rules help to establish and maintain that balance:**

1. The employer should say what personal information it collects from employees, why it collects it, and what it does with it.
2. Collection, use, or disclosure of personal information should normally be done only with an employee’s knowledge and consent.
3. The employer should only collect personal information that’s necessary for its stated purpose, and collect it by fair and lawful means.
4. The employer should normally use or disclose personal information only for the purposes that it collected it for, and keep it only as long as it’s needed for those purposes, unless it has the employee’s consent to do something else with it, or is legally required to use or disclose it for other purposes.
5. Employees’ personal information needs to be accurate, complete, and up-to-date.
6. Employees should be able to access their personal information, and be able to challenge the accuracy and completeness of it.

A. EMPLOYEES PRIVACY RIGHTS VS EMPLOYER’S RIGHT TO MANAGE

Employers have legitimate requirements for personal information about their employees. They need to know who they’re hiring. They need to address performance issues and ensure the physical security of their workplace. And they may see electronic monitoring and other surveillance as necessary to ensure productivity, stop leaks of confidential information, and prevent workplace harassment.

So sometimes employers have to delve into private matters. But they can keep those instances to a minimum, and limit the impact on personal privacy. The possibility that an individual employee might do something harmful doesn’t justify treating all employees as suspects. The questionable benefit of knowing what every employee is doing on company time and equipment, at all times, needs to be weighed against the cost – including the cost to staff morale and trust. Preventing workplace harassment is an important goal, but it’s best achieved through workforce training and sensitization, explicit anti-harassment policies, and appropriate remedial measures when harassment is reported or reasonably suspected, rather than by depriving everyone of their privacy rights.

B. CLEAR POLICIES AND CLEAR EXPECTATIONS

At a minimum, employers should tell their employees what personal information

will be collected, used, and disclosed. They should inform employees of their policies on Web, e-mail, and telephone use, for example. If employees are subject to random or continuous surveillance, they need to be told so.

Employers should also ensure that information they collect for one purpose isn't used for an unrelated purpose without the employee's consent.

Even if they're not required to do so by law, employers should give employees access to the personal information held about them, so that they can verify, and if necessary challenge, its accuracy and completeness.

C. EMPLOYEE WAIVERS

Employers may be tempted to advise employees or prospective employees that they have no expectations of privacy in the workplace – that the loss of privacy is a condition of employment. Someone who agrees to work under these conditions, it could be argued, has consented to unlimited collection, use, and disclosure of their personal information.

Whether this is really consent – clear, informed, voluntary consent – is questionable. And the general principle of collecting only the personal information that's required for appropriate purposes gets lost with this approach. A better alternative is to specifically ask employees to consent to explicit, limited, and justified collections, uses, and disclosures of their personal information.

D. PRIVACY CULTURE

In many workplaces, practices like the ones outlined above are required by law, and employees have legal means to assert their rights. Employees may also have enforceable rights to privacy under collective agreements.

But good privacy practice is not just about avoiding complaints, grievances, or lawsuits. Whether or not privacy is protected by law or contract, fostering a workplace culture where privacy is valued and respected contributes to morale and mutual trust, and makes good business sense.

Workplace privacy is a very complicated area of employment law and can arise in many different situations involving the collection, use and disclosure of private information. Some areas of dispute include employee medical information, the extent to which employers may monitor employees' use of the internet or personal e-mail accounts at the workplace, and the appropriate degree of surveillance over employees at the workplace.

Controversy exists due to a clash of interests. Whereas employees wish to have their privacy rights respected and protected, employers want to ensure that activity in the workplace does not negatively impact their business interests. For instance, internet use could result in non-productive employees who use work computers to spend excessive amounts of working time on social networking sites. On the other hand, an employee who uses the internet during break periods may feel that the employer has no right to monitor the pages visited during non-work time.

E. WORKPLACE PRIVACY GOVERNANCE

Some provinces in Canada have their own statutory legislation to regulate and protect employee's privacy rights. However, no specific legislation currently exists in Ontario, although the *Occupational Health & Safety Act* does provide some protection. Where provincial legislation is lacking, federal legislation does exist, and applies to all federally and provincially regulated employers in all such provinces in varying degrees. The federal legislation is entitled *Personal Information Protection and Electronic Documents Act* and it governs how personal information may be collected, used and disclosed. Common law also governs privacy law in Ontario.

Various court cases have also resulted in common law decisions that may serve as a basis for evaluating workplace privacy disputes. Employers may also have developed their own internal policies outlining the right to collect, use and disclose private information. **The legal enforceability of such policies depends upon many factors, such as the extent to which:**

- the policy is consistently applied in the workplace;
- employers regularly inform employees about the policy;
- employees were involved in creating the policy;
- all employees have a copy of the most updated policy;
- Employees are encouraged to read the policy on a regular basis.

WHY IS EVERYTHING ELSE WRONG

INFORMATION ACCESSIBLE TO THE PUBLIC – IS CONSENT REQUIRED?

In the online environment, the distinction between public and private is often blurred. We often upload our information for the purpose of sharing it with an audience, which can be as small as our family or as large as the whole Internet. Organizations might be tempted to collect personal information that they consider as being public, because it is widely accessible, without obtaining consent.

Under PIPEDA, knowledge and consent for certain purposes are not required when information meets the definition of "publicly available." However, "publicly available information" should not be confused with "information that is accessible to the public." In fact, the definition of "publicly available" under PIPEDA is very restrictive.

PIPEDA Regulations define "publicly available" information as information appearing in telephone directories, professional or business directories, government registry information, and records of quasi-judicial bodies that are available to the public. Generally speaking, no consent is required as long as the collection, use and disclosure of such information **relates directly to the purposes for which it was made publicly available.**

"Publicly available" information also includes information published in a magazine, book or newspaper that is available to the public and where the individual has provided the information.

All personal information that is not "publicly available" as defined above, or which is not covered by the other exceptions, requires consent.

VALID CONSENT

The consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Furthermore, the consent of an employee must be clear, informed, voluntary and meet the common law stringent tests of transparency.

CONSENT IS NOT REQUIRED

PIPEDA contains a list of exceptions for which consent is not required for collection, use, and/or disclosure. The main exceptions to consent are:

1. if the collection and use are clearly in the interests of the individual and consent cannot be obtained in a timely manner;
2. if the collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
3. if disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records;
4. if the disclosure is made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
5. if the disclosure is made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;
6. if required by law.

With regard to consent, if the third party is using the information for the purpose it was originally collected, additional consent for the transfer is not required. Once individuals have consented to do business with a particular company, they cannot refuse to have their information transferred to a third party for processing, as long as the purpose stays the same.

CONSIDERATION IN UPDATING ON–LINE PRIVACY POLICY UP DATES

Organizations should review their privacy policies on a regular basis to ensure that they continue to accurately reflect their personal information handling practices. Privacy policies should be updated as necessary. As a best practice, privacy policies should include the date on which the policy became effective. This will give an indication to users whether the organization is making an effort to keep the privacy policy current.

The privacy policy serves as a mechanism for obtaining users' consent to the organization's privacy practices. Whenever an organization plans to introduce significant changes to the privacy policy, it should notify users in advance and consider asking them to confirm their consent prior to the changes coming into effect. Significant changes include a new arrangement to share personal information with a third party, or using personal information for a new purpose.

As a best practice, organizations should periodically audit their information management practices to ensure that personal information is being handled in the way described by their privacy policy.

ORGANIZATIONS ARE OBLIGATED TO ADOPT CREATIVE DYNAMIC, INTERACTIVE APPROACHES TO OBTAINING CONSENT ON–LINE

It is up to an organization to decide how to obtain meaningful consent in a way that is best suited to its business. However, binary, static and one-time consent mechanisms are often not effective in a fast-paced online environment. Creative options should be explored in order to ensure that approaches to consent are appropriate to the circumstances and that users are in a position to make meaningful decisions affecting their personal information.