info sheet 04.10

Office of the Victorian Privacy Commissioner

Info Sheet 04.10

November 2010

Privacy in the Workplace

Who does this Information Sheet apply to?

This Information Sheet is designed for employers bound by the *Information Privacy Act 2000* (Vic) (**IPA**) – for example, Victorian state government organisations (including local councils, Victoria Police and courts).

The IPA is about *information privacy*: it regulates how Victorian public sector organisations collect and deal with personal information about individuals. "Personal information" is recorded information from which an individual can be identified. Unlike some other jurisdictions such as New South Wales, Victoria does not have a specific Act that deals with workplace privacy. The Victorian Law Reform Commission (VLRC) issued a report on workplace privacy in 2005 which recommended the implementation of a Victorian Act, but as of the date of this Information Sheet, only parts of the VLRC's report have been implemented.[1] Instead, a Victorian public sector employer must abide by the Information Privacy Principles (**IPPs**) under the IPA. Other relevant laws may also apply in different contexts, such as the *Surveillance Devices Act 1999* (Vic) (**SDA**).[2]

Human Resources information

Under the IPA, a Victorian public sector employer can only collect as much personal information as it needs to carry out its functions or activities. An employer should only obtain this information through lawful, fair and not unreasonably intrusive means. The employer should be up front about why the information is being collected, what it is going to use it for, and to whom and to which types of organisations the information is usually disclosed.

In most cases, an employer will need an employee's name, address, telephone numbers and emergency contact details. Employees may also need to provide some of their financial information and date of birth for pay and tax purposes. Some positions require criminal record checks (which *always* need to be conducted with consent); other checks will need to comply with specific legislation such as the *Working with Children Act 2005* (Vic).

[1] Such as the changes to the *Surveillance Devices Act 1999* (Vic) which ban surveillance in workplace toilets, change rooms, lactation rooms and washrooms.

[2] For guidance on privacy obligations and rights at the job application and recruitment stages, see *Information Sheet 02.09: Job Applications, Referee Checks and Privacy*. For guidance on criminal records, see *Information Sheet 03.09: Handling Criminal Records in the Public Sector* (revised).

Depending on the type of position and for processing leave applications, employers may need to collect health information. If this is the case, employers will also need to check their obligations under the *Health Records Act 2001* (Vic) (**HRA**).[3]

If employers require the collection of sensitive information such as race, ethnicity, union membership or criminal record, under IPP 10 an individual must consent or the collection must be required by law. An organisation should be clear about why it is collecting sensitive information and what it is going to do with it. It must also be necessary for one or more of the organisation's functions or activities.

Video camera surveillance

A Victorian public sector employer may install and use surveillance cameras in the workplace in certain contexts, such as security cameras in buildings or foyers, or within reception areas. Usually, cameras will be for safety or security purposes and employees will be caught on camera incidentally.

If an organisation wants to monitor an employee or employees specifically for a purpose other than for security purposes or to protect property, it must show why it needs to collect that information. IPP 1.1 states that an organisation should only collect personal information if it is necessary for one or more of its functions or activities. Collection must also not be unreasonably intrusive, unlawful or unfair (IPP 1.2). In any case, an organisation will need to provide sufficient notice to employees that the video surveillance is taking place in order to comply with IPP 1.3. This may involve the placement of clear signs around the cameras and/or publishing a workplace policy. The policy should be clear about *why* the monitoring is taking place.

To covertly monitor an employee for any purpose, an organisation will require an authorisation or court order under the SDA. The SDA regulates the installation, use and maintenance of surveillance devices such as video cameras (CCTV), listening devices (such as a tape recorder) and tracking devices (such as GPS devices) in Victoria. Victoria Police are responsible for enforcing the SDA. There are probably very few instances where covert surveillance can be justified under the IPA.

The SDA prohibits the installation of surveillance devices in toilets, washrooms, change rooms or lactation rooms in the workplace.

Email and Internet monitoring

(a) Email monitoring

A Victorian public sector employer may need to access an employee's emails for legitimate purposes (for example, monitoring the business emails of an employee when the employee is absent). It may also need access to personal emails to ensure the email system is not misused. Using filtering software to avoid viruses or malware would also be permitted under the IPA.

In any case, an organisation must give reasonable notice under IPP 1.3 to employees as to how information in personal emails will be monitored. Employers should have

[3] See the website of the Health Services Commissioner for more information and contact details at http://www.health.vic.gov.au/hsc/

comprehensive polices on the use of electronic communications which are provided when employees commence work and which are readily available throughout their employment. The policy should specify the acceptable uses of its email system and the situations when the organisation may monitor email usage.

An employer's use of email monitoring to monitor the personal use of email for no purpose other than curiosity may be considered unreasonably intrusive or unfair under IPP 1.2, and will not be necessary (IPP 1.1).

An example of this was seen in *Complainant L v Tertiary Institution* [2004], where the Complainant's emails sent to and from a work email account were copied to the Complainant's Manager without the Complainant's knowledge or consent. The Complainant became aware of this when the Manager went on leave and the Complainant received an "out of office auto reply" from the Manager to an email the Complainant sent to other work colleagues. The Complainant complained to the Privacy Commissioner about the monitoring of work emails by the tertiary institution. The complaint was eventually conciliated, with the tertiary institution apologising, agreeing to advise specified third parties of its failure to inform the Complainant of the monitoring, and giving an undertaking to review its "Use of Electronic Mail Policy".

It should be remembered that the monitoring of employees' email usage may also involve the collection of personal information about third parties. Employers should ensure that the collection of this information also complies with the IPA and relevant IPPs.

(b) Internet monitoring

A Victorian public sector employer that wants to monitor employees' Internet usage should apply the same reasoning as email (above). An employer should only monitor employees' usage where it is necessary to do so (IPP 1.1).

A clearly expressed policy which indicates when and how Internet usage will be monitored should be given to employees. For example, a policy may state that monitoring may occur at any time in order to investigate a suspected violation of the policy (or other organisational policies), to carry out maintenance, to monitor any unauthorised access to the network or to investigate security breaches. While IT administrators may be able to view anything that is stored on or passes over the network for business purposes, they should not abuse these privileges for other purposes such as satisfying idle curiosity about the activities of employees.

An additional web browser warning is a useful way of reinforcing and reminding staff of the presence of the electronic communications policy and that their browsing may be monitored, filtered or logged.

Telephone call monitoring

Where an employer is listening to telephone calls for business purposes – for example, to ensure quality of calls, for coaching purposes or to monitor an employee's performance – this will likely be permitted where it is necessary for one or more of the organisation's functions or activities (IPP 1.1), provided reasonable notice is given under IPP 1.3.

On the other hand, monitoring personal calls will rarely be reasonable or necessary under the IPA. It may be difficult for an organisation to justify why it needs to monitor personal

calls under IPP 1.1. Monitoring calls to satisfy curiosity or other purposes might also be unreasonably intrusive under IPP 1.2.

Workplaces should have policies that govern telephone usage and should take reasonable steps to notify employees and third parties that a particular type of monitoring (such as for performance or coaching) will take place. If personal calls are not allowed, the policy should state this.

The SDA may apply where a listening device is used to monitor telephone calls. Similarly, intercepting telephone calls for certain purposes may fall under the *Telecommunications (Interception and Access) Act 1979* (Cth). Section 7 of that Act prohibits the interception of a communication passing over a telecommunications system (except if an exception applies, e.g. if authorised by a warrant).

Again, monitoring of employees' telephone usage may also involve the collection of personal information about third parties. Employers should ensure that the collection of this information complies with the IPA, relevant IPPs and other laws.

Global Positioning System (GPS) tracking devices

GPS tracking is often used in industries which require employees to drive vehicles by attaching a GPS device to a car. Occasionally, it might also be used to track a person's location. Whether or not the use of GPS tracking is reasonable and legitimate will depend on the circumstances and why this information is needed for the organisation's functions or activities. Employees should be notified when GPS tracking will occur and why this information is being collected.

The use of GPS tracking is regulated under the SDA, which states that the express or implied consent of a person is required to install, use or maintain a tracking device to determine the geographical location of a person. The SDA also prohibits the installation or use of a tracking device to determine the geographical location of an object (i.e. a vehicle) without express or implied consent of the person in control of that object.

Drug and alcohol testing

Testing employees for drugs and alcohol should only be undertaken where it directly relates to a job function and is necessary (IPP 1.1) – for example, where an employee is required to operate heavy machinery or a vehicle and impairment of drugs or alcohol would be a safety risk. Otherwise, it may be unreasonably intrusive or unfair in breach of IPP 1.2.

Employees should be made aware of the implications of failing a drug or alcohol test, the consequences for the individual if they refuse a test, and how the information will be collected, used or disclosed.

The results of a drug or alcohol test may be classed as health information. Accordingly, employers should also check their obligations under the HRA.

Charter of Human Rights and Responsibilities

Public bodies, including public sector employers, are also bound by the *Charter of Human Rights and Responsibilities Act 2006* (the Charter). Section 13 of the Charter contains a right to privacy, which states that "a person has the right not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with".

The right to privacy protected by the Charter is broader than the privacy protected by the IPA. It includes the protection of personal information but also encompasses bodily, territorial, communications and locational privacy. All of these rights may be engaged by some of the forms of employee monitoring discussed in this Information Sheet. Employers should consider whether any such monitoring could be considered unlawful and arbitrary before engaging in it. If in doubt, legal advice should be sought.

IPP1 from Schedule 1 *Information Privacy Act 2000* (Vic)

Principle 1—Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.