Chapter 3
Balancing Employer and Worker Interests

INTRODUCTION

3.1 Chapter 2 has made the case for reform of laws affecting workplace privacy. Privacy is recognised as a basic human right in international conventions to which Australia is a signatory. Promotion and protection of human rights is also one of the Victorian Government’s primary strategic aims. People do not expect to forfeit all protection of their privacy simply because they are working. Rapid advances in technology now allow employers to scrutinise the activities of workers and have access to details of their private lives, to an extent that was impossible in the past.

3.2 The human right of privacy is not absolute. It must be balanced against competing interests, including the interests of employers. Employers have a legitimate interest in reducing their risk of legal liability and in running their businesses efficiently and profitably. When balancing the interests of workers and employers it is also necessary to take account of the inequality of bargaining power that often exists between them. Inequality of bargaining power may place workers under pressure to ‘consent’ to invasions of privacy which cannot be objectively justified. In Chapter 2 we argued that the present law does not adequately balance employer’s interests and workers privacy and that reliance on market forces alone will not address this issue.

1 XX Chapter 2, paras 2.2, 2.3.
2 See Department of Justice Victoria, Department of Justice Strategic Priorities 2005: A Framework for Planning and Opportunities for Collaboration (2005) <www.justice.vic.gov.au> at 5 September 2005, which includes in its top six priorities ‘Justice Statement Implementation’ which contains a ‘major project on human rights’; and Department of Treasury and Finance, Victorian Guide to Regulation (2005) 5-4 <www.vcec.vic.gov.au> at 5 September 2005, which asks whether the objectives of regulation are ‘consistent with Government’s strategic aims’. At 2-2 the guide specifically refers to ‘addressing social welfare objectives’ where ‘in addition to addressing market failure, government intervention can be justified in the pursuit of social and equity objectives’. This includes social policies such as ‘human rights, protecting the vulnerable and disadvantaged’.
3.3 A number of factors must be considered in deciding whether an act or practice undertaken by an employer unreasonably interferes with a worker’s privacy, including the extent of the privacy invasion, the reasons for the act or practice and the workplace context in which it has occurred. For example, it may be reasonable for an employer to require workers doing dangerous work to be regularly tested for alcohol use, but unreasonable for an employer to require a clerical worker to undergo similar tests. Laws which regulate workplace privacy must be able to provide flexible responses which take account of the problems which arise in particular workplaces, while at the same time providing consistency and certainty for both workers and employers. They must also be responsive to developments in technology which have the potential to affect privacy and changes in social attitudes about the use of these technologies.

3.4 As Chapter 2 explains, the proposed legislative model uses a range of mechanisms to regulate acts and practices which have different effects on workers’ privacy. It is intended to:

- provide a fair balance between protecting the human right of privacy and giving employers sufficient freedom to protect their legitimate interests;
- recognise the requirements of different workplaces and different types of work;
- be sufficiently flexible to deal with future developments in the nature of technology and changes in social attitudes to particular practices;
- ensure that acts or practices which affect privacy are proportionate to the interest that the employer is seeking to protect;
- ensure that compliance costs imposed on employers are kept low;
- give adequate protection to workers, without imposing excessive regulation costs on government.

**REGULATORY FRAMEWORK**

3.5 In Chapter 2 we explained our reasons for recommending a regulatory scheme which combines several elements. As mentioned, in developing our proposed scheme we have also taken into account the recommendations contained in the Victorian Guide to Regulation.³

³ Department of Treasury and Finance (2005), above n XX.
LIGHT-TOUCH REGULATION WHERE POSSIBLE

3.6 Regulation which is not intrusive or prescriptive and is cheap to administer and comply with is often described as ‘light touch’. The employers we consulted tended to favour a light-touch regulatory approach. In the context of workplace privacy, light-touch regulation would emphasise the importance of educating employers about privacy protection. It would impose a general obligation on employers to avoid unreasonably interfering with workers’ privacy, rather than setting out detailed rules as to how this should be done. It might also include non-binding codes to assist employers in deciding which practices were in keeping with their broad obligations. Such an approach is consistent with that adopted in the Victorian Guide to Regulation which advocates, where possible, the minimum regulatory measures necessary to achieve the desired objectives.

3.7 The commission agrees with the view expressed by some employers that a light-touch regulatory approach is appropriate to deal with many aspects of workplace privacy. A broad statement of employers’ obligations, combined with advisory codes of practice, will often be the best way of striking a fair balance between their interests and workers’ privacy. Advisory codes can provide guidance to employers about acceptable and unacceptable practices and can be responsive to changing technology, while being sensitive to the issues which arise in different workplaces and to the differing needs of small and big businesses.

STRICHER CONTROLS FOR SERIOUS PRIVACY INTRUSIONS

3.8 Although we support light-touch regulation to deal with most aspects of workplace privacy, we do not believe that advisory codes can provide sufficient protection against some practices which seriously affect workers’ privacy. In the commission’s view, more rigorous controls should apply to acts or practices which affect the privacy of workers when they are not working than those which apply to acts which affect them when they are working. We also propose that stricter controls should apply to activities which are particularly invasive because they affect the bodily integrity of workers (eg drug or alcohol testing) or impinge on their human dignity (eg surveillance of a worker in a toilet or change room). This approach is consistent with the social and equity objectives of workplace privacy regulation and was also supported in a number of employee and employer

---

5 Department of Treasury and Finance (2005), above n XX, 3-3.
6 Ibid 2-2, which classifies ‘social policies’ as including ‘human rights, protecting the vulnerable and disadvantaged’.
submissions. The Victorian Trades Hall Council describes this as, ‘a hierarchy of intrusions some of which require far more stringent testing than others…’.  

3.9 In response to the authorisation model detailed in Option 1 of the Options Paper, the Victorian Automobile Chamber of Commerce’s submission similarly differentiated between practices on the basis of intrusiveness:

if a regulatory system requiring authorisation is implemented, clearly it should be a limited system with only the most intrusive workplace surveillance, monitoring and testing requiring authorisation.

3.10 This acknowledges the fact that the level of intrusion will vary, depending on the practice and the context. The commission’s approach is to ensure the level of regulation matches or corresponds to the level of intrusion. This regulatory approach combines performance-based regulation with more prescriptive measures.

3.11 There is a simple response to concerns about over-regulation in this area. If an employer does not engage in privacy invasive acts and practices regulated by the proposed legislation, then the regulatory impact on the employers’ running of their businesses is nil. Conversely, employers are regulated only to the extent to which they choose to use privacy invasive acts or practices in their business.

**SUMMARY OF PROPOSALS**

3.12 The proposed workplace privacy legislation recommended below has the following features:

- Light-touch regulation will apply to most practices which affect workers when they are involved in work-related activities. The legislation imposes an obligation on employers not to unreasonably interfere with the privacy of workers while they are working. The regulator will have power to issue advisory codes of practice to provide guidance on this duty or to approve codes developed by employers. The codes may indicate how employers should undertake particular activities (eg surveillance in open areas in the workplace) or monitoring email and Internet use over an employer-provided communication system. If a

---

7 Options Paper Submission 28.
8 Options Paper Submission 22.
9 This is consistent with Department of Treasury and Finance (2005), above n XX, 3-87, which refers to ‘performance-based regulation’ as specifying ‘desired outcomes or objectives, but not the means by which these outcomes/objectives have to be met’ in contrast to prescriptive regulation requirements which set out in detail specified, objective criteria and standardised solutions.
worker complains about a privacy invasion, the complaint will not be upheld if the employer has followed a relevant code of practice. Failure to comply with an approved code will be a breach of the employer’s obligation not to unreasonably breach the privacy of workers.

- The regulator will be required to produce codes of practice (mandatory codes) to govern activities affecting workers which are particularly privacy invasive. These include covert surveillance of workers while they are working and taking bodily samples from workers to test for the presence of drugs and alcohol. Failure to comply with a mandatory code will be a breach of the employers’ obligation not to unreasonably interfere with the privacy of workers.

- Some practices which affect privacy will require authorisation in advance by the regulator. Authorisation will be required if the practice affects a person while they are not working, for example out-of-hours surveillance of a worker who is suspected of theft. We argue below that genetic testing is particularly privacy intrusive and should also require authorisation by the regulator. The legislation will allow authorisation requirements to be extended to new technologies which have a significant impact on workers’ privacy.

- Surveillance in private areas in the workplace, for example in toilets and bathrooms, will be prohibited. These are areas in which all members of the community have a very high expectation of privacy. Placing workers under surveillance in these areas would have an unacceptable effect on their human dignity and autonomy.

3.13 The legislation provides for the appointment of a regulator to oversee its operation, undertake education of employers, carry out systemic inquiries and receive and resolve complaints. The regulator’s functions and mechanisms for ensuring compliance with the legislation are discussed in more detail in Chapter 4.

**WORK-RELATED AND NON WORK-RELATED ACTIVITIES**

3.14 As we explained above, the recommended legislation generally gives workers greater privacy protection outside the work context than the privacy protection they will receive when they are working. It will therefore differentiate between the controls imposed on employer practices which affect workers involved in work- as opposed to non work-related activities. This distinction reflects the differing balance between employers’ interests and workers’ expectations of privacy in these two contexts.

3.15 We have used the term ‘activities’ to describe the terms ‘work’ and ‘non-work’ because while the workplace may be a factor in distinguishing the two, it is
not determinative of whether or not work is being performed. Relating the performance of work to activities is more precise than attempting to locate a physical workplace, and more accurately reflects the nature of and liabilities arising from the modern work relationship (see Chapter 1 XX for discussion on the breadth of the modern workplace).

3.16 When workers are performing work employers have a legitimate interest in their activities. For example, employers are entitled to take steps to prevent theft, to protect their intellectual property, to satisfy their occupational health and safety obligations, to prevent sexual harassment of co-workers and to protect third parties from harm, even though the steps they take may have some effect on workers’ privacy.

3.17 Although workers may expect a lower level of privacy at work than in other aspects of their lives, they do not leave their right to privacy at the door. Whether a particular practice achieves a fair balance between workers’ reasonable expectations of privacy and employers’ interests depends on both the purpose for which a particular act is being done and the nature and extent of the privacy invasion. For example, employers may wish to use overt video surveillance in some parts of the workplace to reduce theft of stock. Installation of video cameras in toilet cubicles could reduce the possibility of theft even further, but most employers and employees would regard this as an unjustifiable invasion of workers’ autonomy and dignity. We recommend below that employers should have a legislative obligation not to unreasonably breach the privacy of a worker while the worker is engaged in work-related activities. The concept of ‘reasonableness’ allows a range of factors to be taken into account in balancing employers’ legitimate interests and workers’ privacy. As we explain below, the content of this duty will be clarified in legislative principles.

3.18 When workers’ conduct occurs outside work, it is much harder to argue that the employer has a legitimate interest in their activities. The employer does not have an ‘unfettered right to sit in judgement of out of work behaviour’. Most people expect to be left alone by their employers when they are engaged in non work-related activities. This expectation of privacy should attract a higher standard of protection than the privacy protection to which workers are entitled when they are at work. The fundamental social value underpinning this expectation can be summed up in a comment made at one of our roundtables—a

10 VLRC (September 2004), above n XX, para 3.54.
person can never be someone else’s property.\textsuperscript{12} This is reflected in the NSW Workplace Surveillance Act 2005, which prohibits surveillance when the employee is not at work.\textsuperscript{13}

3.19 The commission’s Occasional Paper Defining Privacy argued that there is a public interest in recognising the privacy of all members of society, regardless of whether they are workers.\textsuperscript{14} This public interest is upheld by protecting the privacy of workers outside the work context. The distinction which the proposed legislation makes between privacy protection inside and outside work is consistent with employment law. An employer’s ability to discipline workers for their after-hours conduct is limited to activities with a direct link to their employment and which have a serious and significant impact on the workplace or employer’s interests.\textsuperscript{15} Similarly, employer liability for discriminatory acts of employees diminishes as the conduct becomes increasingly remote from the work relationship.\textsuperscript{16}

3.20 There are some situations, however, where an employer has a legitimate interest in obtaining information about workers’ activities out of working hours. For example, surveillance of a worker might be necessary to detect fraud or to recover goods stolen from the employer. For this reason, the commission has not recommended a complete prohibition on privacy-invasive practices affecting employees out of working hours. As we explain in more detail below, an employer who wishes to use practices which affect workers out of hours will be required to obtain an authorisation from the regulator.

3.21 The recently enacted NSW Workplace Surveillance Act does not rely on the work/non-work distinction but rather distinguishes surveillance on the basis of whether it is conducted in an overt or covert manner. The commission does not adopt this distinction in our proposed legislation because the practices in our terms of reference are much broader than surveillance and the covert–overt distinction is of little relevance to a practice such as drug and alcohol testing. Consistent with the NSW approach, however, we have used the overt–covert distinction to regulate surveillance, imposing stricter controls on covert than overt forms of surveillance (explained in paragraph XX).

\textsuperscript{12} Roundtable 5.
\textsuperscript{13} \textit{Workplace Surveillance Act 2005} (NSW) s 16. Note this does not apply to computer surveillance, as defined in s 3.
\textsuperscript{14} Foord (2002), above n XX.
\textsuperscript{15} Mary-Jane Ierodiaconou, 'After Hours Conduct' (2004) 78 (4) \textit{Law Institute Journal} 42, 42–45.
\textsuperscript{16} Ibid, for examples of anti-discrimination law cases.
3.22 Our proposed differentiation between practices which affect workers undertaking work-related and non work-related activities makes it necessary to define these terms. Employers need guidance about when workers’ activities are work-related and when they are not because their obligations are based on this difference.

**DEFINITION OF WORK-RELATED ACTIVITIES**

3.23 The definition of work-related activities must take account of the characteristics of the modern workforce. Multiple, global, mobile and cyber workplaces are becoming increasingly common. Workers may do their work at the premises of the employer, in a number of different places outside these premises, or at home. Employers’ health and safety obligations and their potential liability for discrimination and sexual harassment are not limited to situations when workers are on their premises, they also cover workers while they are working elsewhere.

3.24 The recommended definition of work-related activities is loosely based on the ‘at work’ definition contained in the NSW Workplace Surveillance Act. Work-related activities include:

- activities of a worker done in the course of performing work for the employer at the premises of the employer, or at any place other than the worker’s home or residence;
- use of the employer’s communication systems, wherever the worker is located.

The key terms in the definition are explained below.

**PERFORMING WORK FOR THE EMPLOYER**

3.25 Workers’ compensation law imposes obligations on employers when employees are acting ‘in the course of their employment’. Similarly, an employer

---

17 Australian Bureau of Statistics, *Locations of Work* Catalogue No 6275.0 (2000), reports that in June 2000 in their main job, 80% of employed people had worked at their employer or client’s workplace during the week; 31% spent time travelling for work; 20% had worked at their own or a home other than their employer’s or clients; 8% had worked in their own workplace, 5% had worked at their employer or client’s home and 3% had worked in other places, such as forests, parks and streets.

18 *Workplace Surveillance Act 2005 (NSW)* s 5. This Act prohibits covert surveillance of an employee at work for the employer unless the surveillance is authorised by a covert surveillance authority issued by a magistrate.

19 *Accident Compensation Act 1985 (Vic)* s 3, which states the objects to the Act are (a) to reduce the incidence of accidents and diseases in the workplace and (i) in this context, to improve the health and safety of persons at work and reduce the social and economic costs to the Victorian community of
can be liable for torts committed by employees in the course of their employment, and much of employment law is structured around this concept. Because the proposed legislation will cover independent contractors and volunteers as well as employees, our proposed definition refers to the performance of ‘work’ rather than employment. The provision will ensure that when workers are performing activities in the course of their work, at the premises of the employer or elsewhere, acts or practices which affect privacy will generally be governed by the employer’s obligation not to unreasonably affect the worker’s privacy. As we discuss below, guidance on the content of this obligation will be provided by principles in the legislation and by advisory or mandatory codes issued by the regulator.

3.26 Employers often allow workers reasonable work time to undertake personal activities. For example, it may be understood that workers can make reasonable personal use of the Internet to do their banking, make personal travel arrangements, or make some personal phone calls during working hours. These will be treated as work-related activities because they involve the use of the employer’s communication system.

EXCLUSION OF THE WORKER’S HOME OR RESIDENCE

3.27 Except where the worker is using an employer’s communication system, workers’ activities in their home or residence are excluded from the definition of work-related activities. This is the case whether the worker is involved in private activities or performing work for the employer at home.

3.28 The effect of this exclusion is that practices affecting the privacy of workers in their homes will have to satisfy stricter requirements. An employer will be required to obtain an authorisation from the regulator before undertaking activities which affect workers’ privacy in their homes. This requirement reflects the higher expectation of privacy which applies when workers are in their ‘personal space’. It also takes account of the fact that employer acts or practices in the worker’s home have the potential to affect the privacy of visitors to the home.

accident compensation. Section 4 states (1) Despite anything to the contrary in this Act (a) this Act, other than Divisions 6A and 6B of Part IV, applies to and in relation to an injury to a worker on or after the appointed day arising out of or in the course of employment on or after the appointed day.


21 See Breen Creighton and Andrew Stewart, Labour Law (4th ed) (2005) for commentary on ‘in the course of employment’.

22 Ibid272–5. Creighton and Stewart discuss categorisations of work relationships and consider how various legislative frameworks such as OHS and anti-discrimination laws ‘extend beyond the traditional concept of employment in a variety of ways’. It is the commission’s view that this approach lends itself to the broadening of the concept of ‘in the course of employment’ to ‘in the course of performing work’.
or other members of the worker’s family. Employers may be able to justify acts or practices affecting workers at home, but they should have to make a case to the regulator before they can do so.

**WORKERS USING AN EMPLOYER’S COMMUNICATION SYSTEM**

3.29 The definition of work-related activities will include the situation when a worker is using the employer’s communication system, regardless of where the worker is physically located. This means that an employer will not be required to obtain an authorisation before monitoring the worker’s use of the system.

3.30 The rationale for this approach is that employers’ interests are affected by use of an employer-provided communications system, regardless of the workers location or whether the system is being used to perform work- or non work-related activities. For example, an employer may be liable if a worker logs into the employer’s email system from home and uses it to send sexually harassing emails to a co-worker. Employers also have a legitimate interest in preventing their communications systems from being used to download copyright material from the Internet. For this reason, the commission considers that the employer is entitled to treat the use of a communication system as a work-related activity and to monitor use of that system, subject to any applicable advisory codes. This represents an exception to the exclusion of the worker’s home or residence from the definition of work-related activities described in paragraph XX.

**BALANCING EMPLOYERS’ AND WORKERS’ INTERESTS AT WORK**

3.31 The aim of the proposed workplace privacy legislation is to provide a minimum standard of privacy protection for workers without unduly limiting the ability of employers to run their businesses efficiently and competitively. The commission recommends that this aim be achieved by:

- imposing an obligation on employers not to use acts or practices which unreasonably breach workers’ privacy when they are engaged in work-related activities;
- giving guidance on the scope of employers’ obligations by including a statement of general principles in the legislation;

---

23 Along similar lines, the *Workplace Surveillance Act 2005* (NSW) s 16, allows an employer to use computer surveillance of the use by the employee of equipment or resources provided by or at the expense of the employer.

24 *Department of Treasury and Finance (2005)*, above n XX, 3-3.
• providing for the regulator to issue advisory (and in some cases mandatory) codes of practice and to approve codes of practice prepared by employers.

These elements of the regulatory scheme are discussed in more detail below.

EMPLOYERS’ OBLIGATION

3.32 We recommend the legislation should prohibit employers from engaging in acts or practices that might unreasonably breach workers’ privacy. This obligation applies when the worker is engaged in work-related activities. The concept of ‘unreasonableness’ reflects the lower expectation of privacy in the work-related context. The inclusion of this provision qualifies the employers’ obligation by allowing circumstances to be taken into account where employers have a legitimate need to use such acts or practices in the interests of their business. The use of such a concept was supported in a number of submissions, including the Victorian Bar’s:

If a right of privacy is found, the balancing of that right against competing rights or interests should also be based in reasonableness—the relative importance of the two sets of rights, whether there is any way of accommodating the competing rights without the privacy invasion, and if not, which should prevail.26

PROVIDING GUIDANCE ON THE SCOPE OF THE OBLIGATION

3.33 The legislation should provide clarity and guidance to employers and workers on the scope of this obligation. There are a number of ways in which this could be done.

3.34 One way would be to include detailed provisions in the proposed legislation dealing with all the practices which have the potential to affect workers’ privacy. This is rather similar to the approach taken in the NSW Workplace Surveillance Act, which specifies the conditions under which surveillance can be conducted in the workplace.27 We considered whether it would be desirable for the legislation to include detailed requirements for surveillance and Internet and email monitoring. The commission rejected this approach because it would be inconsistent with our preference for using light-touch regulation rather than specific rules, except when dealing with certain practices which have a very serious

25 See Options Paper submissions 23, 24 which, in response to the proposed options in the Options Paper (particularly Option 1), supported the use of a ‘reasonableness test’.

26 Issues Paper Submission 25.

effect on privacy. We were also concerned that provisions dealing with specific practices could rapidly become dated or defunct as a result of technological advances.  

3.35 Another way would be to include broad principles governing particular practices in the legislation. These might be similar to the principles included in existing privacy legislation with which employers are already familiar. This approach was supported by some consultation participants.

3.36 The privacy principles in existing legislation are concerned with the protection of personal information. In our view, it would be difficult to design detailed principles of the kind which protect personal information to cover the broad range of practices which may affect privacy in the context of work-related activities. Instead, the commission recommends the legislation should contain a brief statement of principles, which would be supplemented by more detailed codes of practice issued by the regulator or prepared by an employer or group of employers and approved by the regulator. The approach we recommend has some similarity to that recommended by the New South Wales Law Reform Commission (NSWLRC) in its Interim Report on Surveillance.

3.37 The legislative principles will provide necessary flexibility in applying the employers’ duty not to unreasonably breach the privacy of workers while they are engaged in work-related activities. They will also be able to cover the wide array of workplaces, work relationships and surveillance, monitoring, searching and testing practices and technologies that may be used.

**STATEMENT OF PRINCIPLES**

3.38 A number of submissions commented on possible general principles. One roundtable participant said that principles should be technology neutral and non-practice specific to ensure their ongoing relevance and effectiveness. Some people suggested that general words and expressions in principles such as...
‘acceptable’ and ‘reasonable expectations of privacy’ be avoided or at least defined to give employers guidance about how to comply with the principles.  

3.39 Common themes in discussions were that employers should:

- have a legitimate purpose for which a practice is to be used;
- be required to determine whether less intrusive alternatives are available to the proposed practice;
- ensure that the practices used are proportionate to the risk of harm they are seeking to avoid;
- review their use of practices regularly to determine whether they are still appropriate and necessary;
- consult with workers.  

3.40 These themes were reflected in Allens Arthur Robinson’s submission:

We believe that the principles should encompass the concepts of reasonable expectation, acceptable purpose, proportionality and transparency. These concepts have formed the touchstone of workplace privacy legislation enacted in other jurisdictions both within Australia and overseas.  

3.41 Our proposed principles provide a conceptual framework for balancing the interests of employers and workers by establishing criteria that an employer must meet in using surveillance, monitoring or testing practices or other practices affecting privacy in the workplace.

3.42 As our consultations reflect, the principles represent important societal values and interests in privacy—interests such as legitimacy, proportionality, transparency and accountability which underpin the concept of privacy. It is through the balancing mechanism reflected in the principles that the meaning of an ‘unreasonable’ breach of privacy is clarified for the benefit of employers and employees.

3.43 In the commission’s view, an employer will be in breach of his or her duty not to unreasonably breach the privacy of workers engaged in work-related activities if the relevant acts or practices are used:

- for a purpose not directly connected to the employer’s business;  

---

34 Options Paper submissions 4, 22.
35 See, eg, Options Paper submissions 4, 22, 24; Roundtable 1. In Options Paper Submission 32, an employer proposed that principles should also recognise that organisations can be vicariously liable and can owe a duty of care to their workforce, clients, customers or third parties and that accordingly an employer is entitled to be aware of its workers’ activities.
36 Options Paper Submission 24.
• in a manner that is not proportionate to the purpose for which the practice is undertaken;
• without first taking reasonable steps to inform and consult with workers;
• without providing adequate safeguards to ensure that the act or practice is conducted appropriately having regard to the duty to respect workers’ privacy.

3.44 These principles are broadly drafted to allow employers the necessary degree of flexibility to deal with the diverse situations covered in this report and the different problems which arise in the context of different types of work. We consider each principle below:

Purpose

3.45 Purpose is a fundamental aspect of information privacy regimes. The purpose for which information about an individual is collected generally determines what an organisation can subsequently do with that information. Similarly, a consideration of the purpose for which a practice such as surveillance or email monitoring is used is an important first step in determining whether that practice is justified.

3.46 In our first round of consultations, employers told us why they used video and other forms of surveillance, monitored workers’ email and Internet use, tested them for substances such as drugs and alcohol and used psychological tests in selection or promotion processes. Their reasons included:

• protecting property, including intellectual property;
• minimising legal liability;
• ensuring workers’ health and safety;
• managing worker performance.

37 X-ref to Chapter 1 (where this is covered)
38 Generally, an organisation may use or disclose personal information for the primary purpose for which the information was collected, or for a related secondary purpose which the individual would reasonably expect. See, eg, Privacy Act 1988 (Cth), sch 3, National Privacy Principle 2.1; Information Privacy Act 2000 (Vic) sch 1, Information Privacy Principle 2.1(a); and in relation to health information, Health Records Act 2001 (Vic) sch 1, Health Privacy Principles 2.1(a), 2.2(a).
39 Along similar lines, the NSWLRC proposed in relation to overt surveillance that it should only be undertaken for an acceptable purpose, see NSWLRC (2001), above n XX, 182.
40 VLRC (September 2004), above n XX, ch 3.
3.47 As the practices engaged in to meet these purposes have the potential to invade a worker’s privacy, we recommend the employer should have to show a direct connection between the practice and the operation of the employer’s business. Establishing this connection assists in identifying the legitimacy of the purpose. The commission appreciates that employers are best placed to assess the nature of their particular business and the principle leaves it open to the employer to establish this connection. At the same time, the direct connection requirement offers a degree of protection to workers in ensuring the connection is not trivial or incidental in nature.

3.48 Examples of practices having a direct connection to the employer’s business might be the installation and overt use of surveillance cameras to prevent stock theft, use of an iris scanning device to control entry to the employer’s premises, installing a software system to filter out emails containing trade secrets, or filtering workers’ access to Internet sites to prevent downloading of large files, which will slow the operation of the employer’s system.\footnote{Options Paper Submission 19. In its submission, Clearswift (Internet and email software provider) states that in its research ‘50% of bandwidth is attributed to non-business related information coming into or circulating throughout an organisation’.
} By contrast, regular monitoring of employee emails to ensure that workers are not expressing views contrary to the employer’s religious beliefs or downloading images of workers from a video surveillance camera, simply because the workers are considered attractive, would not comply with this principle.

3.49 Although it will be necessary to show that a practice is directly connected to the operation of the employer’s business, this will not always mean it is reasonable. The principles discussed below will also apply.

Proportionality

3.50 In the context of privacy, the principle of proportionality has been described as providing that ‘any intrusion into an employee’s privacy at work should be in proportion to the benefits of monitoring to a reasonable employer, which in turn, should be related to the risks that the monitoring is intended to reduce’.\footnote{VLRC (October 2002), above n XX, para 5.7, for a further discussion of proportionality.} Accordingly, this principle requires a balancing of the purpose and the effect of the privacy infringement. If that purpose can be achieved in a way which is less intrusive than another act or practice, the employer would normally be expected to use the least privacy-intrusive measure.

3.51 For example, if an employer was considering installing surveillance cameras as a deterrent against theft, under the proportionality principle the
employer would need to consider the least intrusive level of surveillance that would act as a deterrent to dishonest workers. An appropriate level of surveillance might involve setting up cameras at points where stock is most vulnerable and facing cameras towards the stock, rather than always focusing the cameras on workers.

3.52 The principle of proportionality was given importance by both employer and employee organisations. The Victorian Automobile Chamber of Commerce stated in its submission:

It is important to ensure that whatever system is introduced in relation to workplace privacy, it does not further dilute employers’ right to run their businesses as they consider appropriate. Clearly, protecting employee’s privacy is also important, however, the reasonableness test based on proportionality would provide adequate protection.\(^4\)

3.53 The principle of proportionality also assists in engendering trust and confidence in the workplace when measures undertaken by employers are seen by staff as a balanced or measured response to a problem rather than ‘overkill’. This was summed up in the Australian Human Resources Institute’s submission:

The employer would need to think seriously about the benefits of secret surveillance because while, as a police tactic, it might provide a better chance of catching an offender, it can do great damage to workplace trust. Trust is a recurring critical factor in these cases because it is a lack of trust that gives credence to both employer suspicion and employee paranoia.\(^4\)

**Taking Reasonable Steps to Inform and Consult Workers**

3.54 The principle that workers should be informed and consulted about privacy-intrusive acts or practices reflects the fact that privacy is concerned with the protection of autonomy and dignity. Putting practices in place without informing workers about them and the reason the employer wishes to use them denies worker autonomy and is inconsistent with the implied duty not to engage in conduct that would undermine workers’ trust and confidence.\(^4\) Lack of knowledge that a particular practice is occurring also deprives workers of the opportunity to modify their behaviour. For example, workers who are regularly advised that their emails are being monitored may choose not to send personal emails which reveal private matters.

\(^{43}\) Options Paper Submission 22.

\(^{44}\) Issues Paper Submission 16.

\(^{45}\) See VLRC (September 2004), above n XX, para 3.57, for discussion of this duty.
Apart from these principled reasons for informing and consulting workers, there are practical advantages in doing so. Provision of information and consultation with workers will help to educate them about the need to respect the privacy of co-workers and further encourage a healthy, respectful environment. Poor communication between employers and employees about practices which affect privacy may create industrial disputes. A sound consultation process assists in according procedural fairness to workers and is an important part of performance management systems generally. Communication with workers is required in other areas of law, including occupational health and safety law and the federal industrial relations regime.

Informing or notifying individuals is also consistent with the approach taken under existing information privacy regimes, which generally require organisations to take reasonable steps to notify people about their personal information handling practices when or before information is collected (in the context of email monitoring, see, eg, the Australian Privacy Commissioner’s Guidelines on Workplace E-mail, Web Browsing and Privacy).


Options Paper Submission 4. Eg, the Workplace Relations Act 1996 (Cth) requires consultation on an agreement between an employer and a valid majority of the employer’s employees before an agreement is certified: s 170LK(2). The Act requires employers to take reasonable steps to ensure that employees to whom the certified agreement will apply will have 14 days written notice of the intention to make the agreement, and that the agreement must not be made until the 14 days have passed. The employer must take reasonable steps to ensure that those employees have access to the proposed written agreement at least 14 days before approval and to explain the terms of the agreement: s 170LK(3). The notice provided to the employees must state that if the employee is a member of an organisation entitled to represent the employee’s industrial interests, the employee may request that the organisation represent the employee in meeting and conferring with the employer about the agreement: s 170LK(4). The employer must then give that organisation a reasonable opportunity to meet and confer with the employer about the agreement before it is made: s 170LK(5). See also Workplace Relations Act 1996 (Cth), sch 10, art 13, which requires an employer to consult with workers’ representatives when the employer contemplates redundancies for economic, technological, structural or other reasons.

See, eg, Privacy Act 1988 (Cth), sch 3, National Privacy Principles 1.3, 1.5; Information Privacy Act 2000 (Vic) sch 1, Information Privacy Principles 1.3, 1.5; and in relation to health information, Health Records Act 2001 (Vic) sch 1, Health Privacy Principles 1.4, 1.5.

Office of the Privacy Commissioner [Aus], Guidelines on Workplace E-mail, Web Browsing and Privacy (30 March 2000) <www.privacy.gov.au/Internet/email/index.html> at 21 July 2005. The guidelines state: staff and management should know and understand the policy; guidelines should specify what is appropriate use and be explicit about what is and is not permitted; explain what information is logged and who has rights of access with the employer’s operations; set out circumstances for disclosure of information; explain how the organisation intends to monitor and audit staff
3.57 Many employers recognise the importance of transparent processes. A large employer told the commission that it includes information about surveillance, monitoring and testing practices in organisational policies and procedures, induction procedures and in regular communication updates.\(^{50}\) The organisation commented that, ‘We are committed to a transparent approach with our employees in relation to all the practices we undertake, where possible’.\(^{51}\)

3.58 Some people also stressed the importance of incorporating an effective consultation mechanism into the regulatory regime.\(^{52}\) As well as increasing the transparency of workplace practices, consultation may assist employers to identify ways of solving workplace problems that are less privacy invasive than the measures which the employer initially proposes. Consultation does not mean that workers will have a right to veto practices which affect their privacy, but may assist in the formulation of procedures that accommodate more readily the concerns of both employers and workers.

3.59 Employer organisations commented that it may be difficult to consult with workers who are not employees, for example, independent contractors and volunteers who only attend the workplace intermittently. Consultation may also be more difficult where workers are geographically spread. In the case of workplaces with little union representation, it may be difficult for an employer to elicit the views of workers in a manageable way. The requirement of reasonableness provides flexibility in dealing with these issues because it will allow the employer to take account of the composition, size and distribution of its workforce before deciding on a consultation strategy.

3.60 Some employers were concerned that the requirement of consultation might prevent them from using covert surveillance to protect property from theft or to detect a worker engaged in illegal activities. One employer said that informing employees of all surveillance activities could jeopardise a legitimate investigation.\(^{53}\) Paragraphs xx-xx recommend that the regulator should prepare codes regulating use of various types of covert surveillance by employers and that these codes should be binding on employers. The purpose of covert surveillance would be undermined if an employer had to inform particular employees that their activities were being secretly filmed or listened to. In this context, the principle that workers should be informed and consulted would be satisfied by compliance with its policy; and review the policy on a regular basis to ensure it keeps up with technological development and re-issue the policy whenever changes are made.

\(^{50}\) Options Paper Submission 27.

\(^{51}\) Ibid.

\(^{52}\) See roundtables 2, 3, 4, 5; Options Paper submissions 4, 9, 15, 23, 28, 32.

\(^{53}\) Options Paper Submission 27.
informing workers in advance about the situations in which the employer might use covert surveillance and of the safeguards which would apply to its use.

Adequate Safeguards

3.61 This principle requires an employer who wishes to implement surveillance, monitoring and testing practices, to ensure it is done in an appropriate manner. For example, this could require a person conducting a physical search of a worker suspected of theft to be of the same sex as the worker being searched. It could also cover issues such as:

- selection, training and qualifications of the personnel undertaking the practice;
- handling of information obtained from the particular activity (e.g., requiring records of email monitoring to be kept securely so that they can only be inspected by people with a legitimate reason for doing so);
- ensuring the practice is used only for the purposes of which workers have been notified;
- reviewing the use of the practice regularly.

3.62 As we explain in the next section, we envisage that guidance on these issues could be included in codes of practice.

<table>
<thead>
<tr>
<th>RECOMMENDATION(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The legislation should provide that an employer must not engage in acts or practices that unreasonably breach the privacy of workers engaged in work-related activities.</td>
</tr>
<tr>
<td>2. An employer unreasonably breaches the privacy of workers if it engages in acts or practices:</td>
</tr>
<tr>
<td>• for a purpose that is not directly connected to the employer's business;</td>
</tr>
<tr>
<td>• in a manner that is not proportionate to the purpose for which those acts and practices are being used;</td>
</tr>
<tr>
<td>• without taking reasonable steps to inform and consult workers about the relevant act or practice;</td>
</tr>
</tbody>
</table>
20

**RECOMMENDATION(S)**

- without providing adequate safeguards to ensure that the act or practice is conducted appropriately, having regard to the obligation not to unreasonably breach the privacy of the worker.

3. An act or practice is ‘proportionate’ under Recommendation ?? if it is the least privacy-invasive measure by which the intended purpose can be achieved.

4. The obligation to take reasonable steps to inform workers under Recommendation ?? requires provision of information to workers about:
   - the nature of the act or practice and the reasons for introducing it;
   - the number and categories of worker likely to be affected;
   - the time when, or the period over which, the employer intends to engage in the act or practice;
   - the alternatives considered and the reasons why the alternatives were not considered appropriate;
   - the safeguards used to ensure the acts or practices are conducted appropriately.

5. The employer must take reasonable steps to give workers a genuine opportunity to influence the decision to introduce the act or practice.

**CODES OF PRACTICE**

3.63 We recommend that the workplace privacy legislation should provide for codes of practice to be issued or approved by a regulator (the appointment and functions of the regulator are discussed in more detail in Chapter 4).

3.64 There was considerable discussion in submissions and at roundtables about how codes could regulate workplace privacy. There were also differences of opinion about whether failure to comply with a relevant code should be regarded as a breach of the employers’ duty not to unreasonably breach the privacy of workers (in which case compliance with the code would be mandatory), or whether codes should only be used to give employers non-binding guidance on how to meet their privacy obligation. There were mixed views on this issue among employers.
3.65 Some employers and employer organisations favoured advisory codes because they thought they would not impose excessive compliance costs and would provide guidance to employers without fettering their right to manage their workers. It was also argued that use of advisory codes was consistent with the approach taken to regulation in areas such as information privacy and workplace bullying.

3.66 Unions were more likely to support mandatory codes of practice because of concerns that a ‘softer’ form of regulation would provide insufficient privacy protection to workers and place too much emphasis on employer perspectives and interests.

3.67 Our recommendations will allow the regulator to issue advisory codes covering most practices affecting workers. However, we also recommend the use of mandatory codes to regulate acts or practices which are particularly intrusive because of their effect on workers’ autonomy and dignity.

**Advisory Codes**

3.68 We have recommended that employers should be under a duty not to engage in acts or practices that unreasonably breach a worker’s privacy, and that the content of this duty should be determined by reference to four broad principles. We believe the regulator could provide guidance to employers by issuing advisory codes which clarify how various acts or practices can be undertaken in a way which complies with this obligation. Advisory codes could be drafted in a way which takes account of the needs and characteristics of different practices, different industries and different workplaces (e.g. the differences between small and big business). This approach allows the minimum regulation necessary to fulfil the social objective of privacy protection, while maximising business competitiveness and reducing possible administrative burden. Of course, the

54 See Options Paper submissions 8, 15, 20, 24.
55 Roundtables 3, 4.
57 Roundtable 3. See also Options Paper Submission 4.
58 Options Paper Submission 28.
59 Department of Treasury and Finance (2005), above n XX, 3-3.
obligation and principles would continue to apply to employers regardless of whether a code is issued.

3.69 Under our recommendations, advisory codes could be issued covering practices such as email and Internet monitoring, psychological and medical testing of workers, use of biometric measures to control entry into buildings and the searching of workers and their belongings. Our recommendations will allow overt surveillance to be dealt with under an advisory code, but covert surveillance will be subject to stricter controls, which are discussed below.\(^{60}\)

3.70 Issuing advisory codes is similar to the approach taken under many information privacy regimes. For example, the Federal Privacy Commissioner has issued guidelines to help organisations comply with the National Privacy Principles contained in the Privacy Act 1988. The guidelines include factors which the Privacy Commissioner may take into account when handling a complaint, but are advisory only and not legally binding.\(^{61}\) A similar approach is taken in the United Kingdom.\(^{62}\)

3.71 Where the regulator has issued an advisory code and the employer has complied with it, we recommend this be conclusive evidence of compliance with the legislation and a sufficient answer to any complaint made about a breach of privacy. This is similar to the approach taken under the Victorian Occupational Health and Safety Act 2004.\(^{63}\) Employers who have failed to comply with an advisory code issued by the regulator will be regarded as being in breach of the legislation, unless they can show they have taken other steps to comply with their obligation not to unreasonably affect workers’ privacy.

3.72 As well as the regulator having power to issue advisory codes, we recommend it should have power to approve codes of practice developed by

---

\(^{60}\) See x-ref below.


\(^{62}\) In the UK, employers are required to comply with the provisions of the Data Protection Act 1998. The UK Information Commissioner has issued a code which sets out good-practice recommendations for employers on conducting workplace surveillance and monitoring. Any enforcement action would be based on a failure to meet the requirements of the Act. However, relevant parts of the code are likely to be cited by the commissioner in connection with enforcement action. If an employer breaches the Act, compliance with the code can assist with the employer’s defence: see Information Commissioner’s Office, The Employment Practices Data Protection Code (2005) 6.

\(^{63}\) See Occupational Health and Safety Act 2004 (Vic) ss 149–152.
employers (or employer representative organisations) provided that these codes comply with the principles set out in Recommendation 2. x-ref. For example, there may be scope for the retail industry to develop a retail video surveillance code, or the transport industry to develop codes on GPS tracking or drug and alcohol testing. Where the code has been produced by an employer and approved by the regulator, failure to comply with the code will be a breach of the employer’s obligation not to unreasonably breach workers’ privacy.

**APPLICATION OF ADVISORY CODES TO JOB APPLICANTS**

3.73 Job applicants are frequently required to have medical examinations or submit to psychological tests. Employers argue that these tools can assist in eliminating bias by increasing objectivity in assessments of people who are applying for a job. Such tests are meant to ensure that decisions are based on the ability to meet the requirements of the job and not on other irrelevant, or potentially discriminatory, factors.

3.74 Where information sought is directly relevant to the position, job applicants cannot legitimately object to practices which enable the employer to assess whether they are capable of performing the job on offer. However, the commission’s Options Paper referred to a number of problems with psychological testing, including the use of inappropriate tests and their administration by people lacking relevant qualifications. While psychological tests may sometimes be useful, there are no legal requirements that ensure they will provide reliable information or be administered in an appropriate way. Job applicants may be required to answer invasive questions about private matters such as their social habits, likes and dislikes which have little or no relevance to their capacity to do the job.

3.75 The Victorian Trades Hall Council limits its support of pre-employment testing to testing which relates directly to the skills required to perform the job. Other unions advocate a total ban on pre-employment psychological and pre-disposition testing.

---

64 The recommendations also apply to other prospective workers, eg, people seeking a voluntary position.
66 VLRC (September 2004), above n XX, paras 2.38–2.92.
67 Consultation 4.
68 Options Paper Submission 28.
69 See Options Paper Submission 31; Roundtable 2.
3.76 The commission believes there are legitimate uses for reliable tests which provide employers with information directly relevant to the performance of the job. But this must be balanced against the job applicant’s right to protection against practices that unreasonably invade their privacy. People applying for a job are likely to find it difficult to refuse testing, even though the test has little relevance to their suitability for employment. For this reason, we recommend that the regulator’s power to issue advisory codes dealing with use of medical and psychological tests should apply to job applicants and other prospective workers, as well as to people who are already working for the employer.

3.77 Later in this chapter, we make recommendations about drug and alcohol testing and the use of genetic information with respect to job applicants and other prospective workers.

<table>
<thead>
<tr>
<th>RECOMMENDATION(S)</th>
</tr>
</thead>
</table>
| 6. The regulator should have the power to publish advisory codes of practice to provide practical guidance to employers about how to fulfil the obligation imposed by Recommendation ??.
| 7. Advisory codes may cover acts or practices which affect the privacy of workers while they are engaged in work-related activities other than:
  - acts or practices to which mandatory codes apply under Recommendation ??;
  - acts or practices which require authorisation under Recommendation ??;
  - acts or practices which are prohibited under Recommendation ??.
| 8. An advisory code of practice prepared by the regulator must be consistent with the principles in Recommendation ???.
| 9. Compliance with an advisory code is conclusive evidence that the employer has complied with the obligation imposed by Recommendation ??.

---

70  Eg, people applying for internships or other voluntary positions.
71  See paras X (drug and alcohol testing) and paras X (genetic testing).
10. If an advisory code is in operation, contravention of the code is a contravention of the obligation imposed by Recommendation ?? unless the employer complies with that obligation in some other way.

11. The regulator should have power to approve codes of practice (approved codes) prepared by employers dealing with acts or practices which affect the privacy of workers while they are engaged in work-related activities, other than:
   - acts or practices to which mandatory codes apply under Recommendation ??;
   - acts or practices which require authorisation under Recommendation ??;
   - acts or practices which are prohibited under Recommendation ??.

12. The regulator may only approve a code which is consistent with the principles set out in Recommendation ??.

13. An employer must comply with an approved code of practice.

**Mandatory Codes**

3.78 Although we believe light-touch regulation is the best method of regulating most practices affecting employees engaged in work-related activities, there are some practices which may have such a serious effect on privacy that they require stricter controls. We recommend that the regulator should be required to issue codes regulating certain practices and that employers should be required to comply with these mandatory codes.

3.79 Which practices should be covered by mandatory codes? Our Occasional Paper *Defining Privacy* noted that the feelings of individuals vary widely as to whether particular activities amount to serious invasions of their privacy. The answer to this question may differ according to the person’s culture, the situation in which a practice occurs and the circumstances in which workers perform their
jobs. For example, a retail shop assistant, whose activities are observed by customers, may have different expectations of privacy from workers in an office on their own. But the existence of these differing expectations is not an argument for failing to protect privacy. Defining Privacy argued that there is a public interest in protecting human beings from activities which undermine workers’ autonomy and dignity, because such activities undermine their status as human beings.

3.80 This concept of public interest underpins the distinction we have drawn between activities which may be regulated by use of advisory codes and those which require stricter controls, or which should be prohibited altogether. The commission recommends that the legislation should require the regulator to issue codes covering:

- use of covert surveillance;
- taking of bodily samples from workers or prospective workers for the purpose of testing for the presence of alcohol and drugs.

It should be possible for other practices to be prescribed by regulation so they are also regulated by mandatory codes. Breach of a provision in a mandatory code will be regarded as a breach of the legislation.

3.81 Sometimes use of these practices will be disproportionate to the goal which an employer is seeking to achieve. However, we recognise that in some limited circumstances an employer may have legitimate reasons for using them. Mandatory codes could control the way in which these practices are undertaken, so as to provide an appropriate balance between protecting the interests of employers and the privacy of employees.

Covert Surveillance

3.82 Under Recommendation x-ref overt surveillance (that is, surveillance with the worker’s knowledge) will have to be conducted in accordance with the general principles set out in the legislation. The regulator may also issue advisory codes as to how various types of overt surveillance should be conducted. In the following paragraphs we explain why we propose stricter controls for covert surveillance.

3.83 By covert surveillance we mean video surveillance, use of a listening device such as a tape recorder, tracking technology such as a GPS device and

---

73 Ibid.
74 Foord (2002), above n XX, 40.
75 These terms are defined in the Surveillance Devices Act 1999 (Vic) s 3.
monitoring of email or Internet use that is undertaken without a worker being notified of the surveillance. For example, covert video surveillance occurs when an employer films a worker on a hidden camera without informing the worker of the surveillance. Covert email surveillance occurs when emails sent or received by workers are monitored without workers being aware it is occurring.

3.84 The issue of whether covert surveillance should be treated differently from overt surveillance attracted some comment in submissions and at roundtables. Some unions argued that both overt and covert surveillance can be objectionable, depending on the context. 76 Concerns were expressed about the increasing use of overt surveillance to monitor workers’ productivity. We were told this was becoming pervasive in some areas of work, such as call centres. 77 Unions said overt surveillance was being used as a substitute for good staff management and it reduced trust in the workplace and contributed to worker stress and breakdown. 78 On this basis, unions argued that both overt and covert surveillance had the potential to severely affect workers and that notifying a person that surveillance was being used did not reduce this effect. 79

3.85 The commission believes some concerns about excessive use of overt surveillance are justified and this use can severely affect workers’ autonomy and dignity. The regulator will have power to publish advisory codes governing this kind of surveillance. In our view, however, the use of surveillance generally to monitor and increase workers’ productivity raises issues about working conditions which are not limited to the protection of workers’ privacy. It may be preferable to deal with conflicts about intrusive productivity monitoring within a broader industrial relations framework, rather than simply as a privacy matter. 80 In Chapter 4 we propose that the regulator should have power to decline a privacy complaint if it would be more effectively dealt with in another forum.

76 Roundtable 2.
77 See, eg, Roundtable 5, consultations 15, 6, 21.
78 See, eg, Issues Paper Submission 2, in which the Australian Honesty Forum states, ‘surveillance can impinge on mental, rather than physical, health. When employees are monitored, they feel the need to suppress their emotions and opinions continuously. They fear the expression of their genuine feelings could jeopardise their position or status. This continuous suppression of emotions and opinions tends to induce burnout—a sense of mental exhaustion and alienation’. In Issues Paper Submission 5, a former call centre worker said ‘I found this to be an extremely stressful environment and eventually the pressure got to me and I could no longer continue. Many other people I spoke to found it stressful to be monitored so heavily’.
79 Options Paper Submission 5.
80 An example of this is the use of ‘mystery shoppers’. This practice was raised as a privacy issue on a number of occasions during our consultations, but has more to do with the use of a particular kind of performance-management practice than an issue of workplace privacy: Consultation 6
3.86 Other stakeholders thought that covert surveillance should be subject to some kind of authorisation mechanism because it was more intrusive than overt surveillance.\(^81\) It was suggested that employers should not have greater powers to undertake covert surveillance than the police, who are generally required to obtain a warrant to undertake such activities.\(^82\) It was also suggested that if employers suspect unlawful activity they should be required to seek police assistance rather than trying to catch the perpetrators themselves. Employers thought this would create difficulties as the police may not have the time and resources to investigate all suspected activities. Employers were also concerned that having to seek some kind of authorisation before using covert surveillance could lead to loss of evidence due to potential delays in obtaining an authorisation.\(^83\)

3.87 On balance, the commission believes it should be permissible in limited circumstances for employers to engage in covert surveillance of workers, but it should be more strictly regulated than overt surveillance because of the more intrusive effects on workers’ autonomy. For this reason, we recommend it should be controlled by mandatory codes. Covert video surveillance may capture workers engaged in a private activity (such as blowing their nose, scratching a body part or changing clothes while in a company-provided car). Covert email monitoring may result in employers becoming aware of matters which have no relationship to workers’ responsibilities (eg matters about their health, sexual orientation or intimate relationships). If workers know they are being watched they have the chance to modify their behaviour and so control the way they present themselves to the world. Similarly, workers who know their emails are monitored can decide not to send emails dealing with private matters. Another reason for placing stricter controls on covert surveillance is that it can affect the privacy of people other than workers. For example, covert email monitoring affects the privacy of a person to whom the worker sends the email as well as of the worker. Likewise, covert use of video surveillance affects people who visit the workplace.

3.88 The NSWLRC has pointed out that covert surveillance may discriminate against groups such as low paid workers, who are more likely to be its targets, and it may also result in the targeting of ‘certain individuals or groups’, such as union members.\(^84\) In NSW the need to control covert surveillance has been recognised by

---

\(^{81}\) Roundtable 3; Options Paper submissions 4, 14, 30, 32.
\(^{82}\) Roundtable 5. See, eg, Surveillances Devices Act 1999 (Vic) pt 4, which sets out the requirements in relation to warrants for the use of surveillance devices by law enforcement officers.
\(^{83}\) Roundtable 5.
\(^{84}\) NSWLRC (2001), above n XX, 287.
legislative provisions which require authorisation to be obtained from a magistrate before surveillance is undertaken.\(^{85}\)

3.89 The commission considered the NSW approach of requiring an employer to obtain authorisation from a magistrate before using covert surveillance.\(^{86}\) However, we believe requiring employers to comply with mandatory codes on surveillance is a more appropriate way of achieving the necessary balance between the interests of employers and protecting the privacy of workers. The NSW requirement of obtaining an authorisation from a magistrate deals with covert surveillance on a case-by-case, rather than systemic basis. In our view, mandatory codes are more likely to produce a systemic change in employer practices. They can deal with issues such as:

- the purposes for which covert surveillance may be used;
- qualifications of personnel undertaking the surveillance;
- the manner in which covert surveillance is conducted;
- secure storage and handling of the results of surveillance (such as video surveillance tapes).

3.90 The commission therefore recommends the regulator develop codes for different types of surveillance. For example, there might be a code for covert video surveillance and a code for covert tracking.

**Drug and Alcohol Testing**

3.91 Drug and alcohol testing is now used in a number of industries in Australia, although there are no recent statistics on the extent of its use.\(^{87}\) Some organisations which made submissions or attended roundtables said that such testing should be prohibited, or only allowed in specified situations.\(^{88}\) The commission does not support an outright prohibition of these practices as it believes their use may be justified in some situations for occupational health and safety reasons. This is particularly so given the inclusion of drug and alcohol testing in... 

---

\(^{85}\) *Workplace Surveillance Act 2005 (NSW).*

\(^{86}\) See Office of the Attorney General NSW, *Report by the Attorney General of New South Wales of Applications Pursuant to Section 26 of the Workplace Video Surveillance Act 1998 for the Year ended 31 December 2004* (tabled 21 June 2005, Legislative Assembly)—in 2004, 103 applications were made for the issue of an authority allowing covert video surveillance. Incidences were reported to police in 13 cases. No unlawful activity was detected in 10 cases. The authority was terminated/not exercised in 7 cases. The employee resigned/was dismissed in 3 cases.


\(^{88}\) In Roundtable 5 it was suggested drug and alcohol testing should be prohibited with exemptions for particular cases such as drug testing of airline pilots.
testing programs in some federal industrial agreements (which have the force of federal law). In the commission’s view, drug and alcohol testing should be subject to mandatory codes. Stricter control of these practices is necessary because of their invasiveness, the potential for misuse of information obtained from them and the varying reliability of these tests.

3.92 The process of drug and alcohol testing is inherently intrusive because it involves the taking of bodily samples. The most common forms of testing involve breath testing for alcohol and urine testing for drugs. The taking of saliva samples is also becoming common. Blood testing may be required to confirm the results of other less accurate tests. Privacy is often characterised as relating to an individual’s autonomy and dignity and the concept of bodily privacy is integral to this. Taking bodily samples erodes the distinction between the privacy of workers’ bodies and the obligations they owe to their employers. There is nothing except the cost of testing to stop employers requiring workers to submit to weekly tests of their urine, blood or saliva as a condition of employment. The results of these tests may have little or no relevance to workers’ capacities to do their job. Many unions objected to random drug and alcohol testing. The Shop, Distributive and Allied Employee’s Association said in their submission that ‘testing must be incident based, not random and should only relate to impairment’.

3.93 Another reason for applying mandatory codes to drug and alcohol testing is that these tests can provide a great deal of private information. Drug testing in particular has the potential to reveal information about a worker’s private life. Such tests might, for example, reveal that a worker is taking prescription drugs to treat a particular disease, which the worker wishes to keep private and which may be irrelevant to his/her capacity to do the job.

3.94 Tests may also reveal that workers have taken a recreational drug in their own time. Unions have expressed concern that employers might act as ‘de facto police’ in monitoring workers’ drug and alcohol consumption after hours, when it may have little or no effect on their work performance.

89 See VLRC (September 2004), above nXX, para 2.90.
91 Options Paper Submission 9.
92 See VLRC (September, 2004), above n XX, paras 2.72–92 for a discussion about the processes of drug and alcohol testing.
3.95 Finally, the reliability of these tests also varies. The process of drug and alcohol testing is largely unregulated and there is no requirement on the employer to put steps in place to ensure the accuracy of the test or to require bodily samples to be analysed by an accredited laboratory.  

3.96 Matters which should be addressed in the mandatory code include:

- the need for written consent from the worker;
- what kind of tests should be used;
- the purposes for which tests may be used;
- whether testing is for a specific reason or is random;
- how tests should be conducted;
- what substances may be tested for;
- the qualifications of the personnel who conduct the tests;
- the accreditation status of laboratories used to analyse the tests;
- secure storage and handling of any samples taken;
- cross reference made to information privacy requirements contained in the Health Records Act.

Other Prescribed Practices

3.97 Technology is evolving at a rapid rate and community attitudes to particular practices change over time. For these reasons, the commission believes the proposed legislation should contain a provision enabling other practices to be regulated by mandatory codes. We recommend the legislation allow regulations to be made requiring other practices to be covered by mandatory codes prepared by the regulator. Such new practices may come to light through the complaints system or through the regulator’s investigation powers, which are discussed in Chapter 4. In that chapter we recommend one of the regulator’s functions be to monitor technological developments to assess the impact on worker privacy. This is also consistent with the Victorian Guide to Regulation requirement that regulation should be constantly evaluated to ensure that the specified social and equity objectives are being met.

3.98 Another rationale for enabling other practices to be regulated by mandatory codes is that it provides a safeguard if employers do not follow their

---

94 See VLRC (September, 2004), above n XX, paras 2.74, 2.77, 2.92, which discuss accreditation of laboratories in relation to drug and alcohol testing. For further discussion of issues in drug and alcohol testing, see ibid paras 2.72–2.92, 3.52–3.101.

95 Department of Treasury and Finance (2005), above n XX, 3-3.
advisory code obligations. If employers fail to meet their obligations under the light touch regulatory regime, the practice in question may be prescribed by the regulator and made subject to more onerous/mandatory regulation.

3.99 As these codes have mandatory effect, the legislation includes an important transparency measure. The issuing, variation or revocation of a mandatory code of practice must receive approval by the relevant minister.

3.100 One practice which may be worth monitoring is the potential use of radio frequency identification (RFID) chips to track or monitor individuals. It was recently reported that the US Food and Drug Administration had approved the use of RFID chips for use in hospital patients to facilitate patient care. The chips can be injected into the fatty tissue of patients’ arms and a scanner can be used to obtain information about their blood type, identity and condition.

3.101 Although RFID technology is used in Australia, the commission is not aware of its use to track the location of workers. It would be possible to track a worker’s every movement by including an RFID chip in clothing which is required to be worn at work. Regulation could require mandatory codes to be prepared to govern use of RFID if employers began to use this technology to track workers’ movements.

Job Applicants and Other Prospective Workers

3.102 The commission recommends mandatory codes for drug and alcohol testing cover testing of job applicants and others who are seeking positions as independent contractors or volunteers (prospective workers), as well as people who are already workers. This is because a job applicant or other prospective worker may be placed in the position of consenting to a privacy invasive act or practice or missing out on the job altogether. This issue was identified in the report of the Privacy Committee of New South Wales into workplace drug testing, which

---

96 Another practice that may also be worth monitoring is x-ray scanning machines that can see through clothing. It has been reported that Sydney airport is keeping a close eye on overseas trials of the technology; see Neil McMahon, ‘Airport security could get a little more intimate’, Sydney Morning Herald (NSW), 27 July 2005.

97 RFID, or radio frequency identification, ‘is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached or incorporated into a product. RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transponder’: <http://en.wikipedia.org> at 5 May 2005. RFID is typically used to tag and identify mobile objects such as consumer goods, postal packages and sometimes even pets: author, title (date), organisation <www.computer-networking.miningco.com> at 5 May 2005.

acknowledged that consent is virtually meaningless in the pre-employment context. Evidence of the difficulty which job applicants face in refusing a test was reflected in an employer representative’s comment to the commission that there was generally no resistance to pre-employment testing.

3.103 For this reason, the commission recommends that an employer wishing to drug and alcohol test job applicants should have to comply with a mandatory code of practice issued by the regulator. This approach allows employers to continue to use such testing for legitimate purposes, while the mandatory nature of the code attempts to ensure this particularly vulnerable group is provided a guaranteed level of privacy protection. As the processes involved in drug testing and alcohol testing are different, the commission recommends that a separate code be developed for each.

<table>
<thead>
<tr>
<th>RECOMMENDATION(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. The regulator must issue mandatory codes of practice about the following acts or practices:</td>
</tr>
<tr>
<td>• covert surveillance of workers in the workplace (including covert use of optical surveillance devices and of listening or tracking devices and covert surveillance or monitoring of emails or Internet use);</td>
</tr>
<tr>
<td>• the taking of bodily samples from workers or prospective workers for the purposes of drug and alcohol testing;</td>
</tr>
<tr>
<td>• any other acts or practices that are prescribed by regulation for the purposes of this section.</td>
</tr>
<tr>
<td>15. A mandatory code of practice must be consistent with the principles in Recommendation ??,</td>
</tr>
<tr>
<td>16. In deciding whether to issue a mandatory code the regulator should consult with relevant organisations and persons.</td>
</tr>
</tbody>
</table>

100 Consultation 10.
RECOMMENDATION(S)

17. A mandatory code of practice, or a variation or revocation of a mandatory code of practice, must be approved by the relevant minister.

18. An employer who fails to comply with a mandatory code breaches the obligation imposed by Recommendation ??

PRIVACY PROTECTION FOR WORKERS WHEN NOT WORKING

3.104 Recommendations ?? to ?? are intended to balance the interests of employers and the privacy interests of workers when they are involved in work-related activities. We argued in XX–XX that workers should receive greater privacy protection when they are not working.

3.105 Because workers are not ‘owned’ by their employers, they have the same privacy interests when they are not working as everyone else. The fact that a person is an employee, an independent contractor or a volunteer should not qualify a reasonable expectation of privacy outside the work context. As the Privacy Committee of NSW has commented, ‘it is important for people to be able to preserve a distinction between their public and private worlds’.

3.106 It follows that employers should not normally use acts or practices which affect workers’ privacy when they are not working. The commission’s Occasional Paper Defining Privacy argued that privacy is not just a matter of individual concern but a condition of existence as a human being. Interference with workers’ rights to enjoy a social life outside work erodes their humanity and treats them as if they are owned by their employers. For this reason, it will usually be inconsistent with the public interest to allow employers to attempt to monitor the activities or movements of a worker outside working hours. There is little evidence of the extent to which this is currently occurring, but during the course of the reference we were given some examples. For instance, we were told that private detectives were sometimes hired by reputation-sensitive employers to place executive workers under surveillance to discover whether they were having an affair, or to ascertain whether a worker was selling property stolen from the employer.

101 Privacy Committee of New South Wales (1995), above n XX, 41.
102 Foord (2002), above n XX, 40.
3.107 Although employers should not normally use acts or practices which affect the privacy of workers outside work, we do not think the complete prohibition of such practices is justified. Some incursion into workers’ lives may be warranted when a worker does something outside work that has a direct effect on work responsibilities. For example, the fact that a member of the police force is associating with criminals out of hours or that a teacher is having a sexual relationship with an under-age student is directly relevant to their work. Where such behaviour is suspected, it may be legitimate for an employer to put measures in place to determine whether these acts are occurring.

3.108 There are also situations where it is practically impossible to use technologies which affect the worker’s privacy in the context of work, without also having some effect on the worker’s private life. For example, an employee may be provided with a car to be used both for work and private purposes. The car may have a GPS device installed in it, which enables the employer to track the worker’s movements out of hours as well as during working hours. There may be difficulties in ensuring that the device is deactivated at times when the worker is not working. In this situation it may be preferable to place conditions on access to and use of information about the worker’s out-of-hours movements, rather than preventing use of GPS devices altogether.

3.109 Our approach begins with the assumption that it is an important social objective that employers should not invade a worker’s privacy when the worker is not working. Where the employer argues there is a justification for doing so, the employer should be required to displace this assumption and show that the act or practice is proportionate to the protection of the employer’s interest, having regard to the higher expectation of privacy which workers have in relation to their private lives.

103 Issues Paper Submission 12. The Department of Education and Training raises the issue of teachers’ out-of-hours conduct, ‘In the teaching profession, off-duty personal conduct may amount to misconduct. The reason for this is that a teacher holds a position of trust, confidence and responsibility. If he or she acts in an improper way, on or off the job, it may demonstrate that the teacher lacks good character and is unfit to practise as a teacher, there may be a loss of trust and public confidence in the teacher and the public school system, a loss of respect by students for the teacher involved, and other teachers generally, and there may be controversy within the school and within the community which disrupts the proper carrying on of the educational system’.

104 An argument against using a ‘public/private’ distinction as the conceptual basis for the model is the underlying assumption that greater privacy protection attaches to the ‘private domain’ even though certain ‘public acts’ may warrant a high degree of privacy protection (for a general discussion of these concepts see Foord (2002), above n XX, 38–41 and Victorian Law Reform Commission, Privacy Law: Options for Reform (2001) paras 3.1–3.25). The proposed workplace privacy legislation moves beyond the parameters imposed by the public–private distinction by relying instead on whether or not work is being performed. This approach reflects the complex nature of the modern work
AUTHORISATION REQUIREMENT

3.110 We recommend that the employer should be required to apply to the regulator for an authorisation in situations where the employer proposes to invade workers’ privacy when they are not working.

3.111 The authorisation process will require the employer to ‘build a case’, and demonstrate to the regulator the need for such an act or practice (eg why an employer wishes to log GPS tracking of company-provided cars outside of work hours, or why the employer needs to place an employee suspected of theft under after-hours surveillance).105 The regulator may authorise the act or practice if satisfied that:

- the worker’s out-of-hours activity has the potential to have a direct and serious impact on the business or reputation of the employer;
- the act or practice affecting privacy cannot reasonably be undertaken while the worker is engaged in work-related activities;
- there is no other reasonable way of protecting the employer’s interests;
- the effect of the act or practice on the worker’s privacy is proportionate to the protection of the employer’s interests, having regard to the higher expectation of privacy which applies to workers when they are not working;
- the employer will ensure the act or practice is conducted appropriately;
- adequate safeguards have been put in place to minimise the interference with the worker’s privacy.

3.112 These criteria give employers guidance on what they must demonstrate to the regulator in seeking an authorisation, and make transparent the factors which the regulator will take into account in authorising the act or practice. The criteria will also contribute to the development of minimum standards to protect workers’ higher expectation of privacy in the non work-related context. Where an employer engages in an act or practice in the non work-related context without an authorisation, a civil penalty applies (see para XX for further detail). One of the regulator’s functions (see para XX for functions of regulator) is to issue guidelines to assist employers in preparing for an authorisation. We believe, given the

---

105 Roundtables 1, 2.

relationship which traverses both public and private domains. The performance of work can, for example, occur in the so-called private domain of the home. Conversely, highly privacy-invasive activities can occur in the public domain of the workplace. Accordingly, the prescribed level of regulation is not determined by whether the act occurred in the public or private domain, but rather focuses on whether or not work is being performed (assessed against other considerations such as the degree of the privacy invasiveness of the practice).
Balancing Employer and Worker Interests

seriousness of the social objective at stake, this form of regulation is justified to ensure the desired regulatory outcome.\textsuperscript{106}

**DRUG AND ALCOHOL TESTING**

3.113 We have recommended that drug and alcohol testing of workers involved in work-related activities should be regulated by mandatory codes. There are some situations where an employer may wish to monitor the drug intake of a worker when they are not working. Some sporting organisations are required to randomly drug test athletes in order to meet international requirements for sporting events.\textsuperscript{107} Sporting and other organisations may also argue that they are entitled to ‘protect their image’ by monitoring athletes’ or workers’ drug or alcohol consumption outside the work context.\textsuperscript{108} Workers may be placed under pressure to consent to monitoring at times when they are not working.

3.114 While this form of monitoring will often unreasonably interfere with workers’ privacy, there may be some situations where it is justified. Our recommendations mean that an employer will have to obtain an authorisation from the regulator for drug and alcohol testing outside the context of work-related activities. As we discuss in Chapter 4, the employer will be able to seek a Victorian Civil and Administrative Tribunal (VCAT) review of a decision made by the regulator to refuse an authorisation.

<table>
<thead>
<tr>
<th>!</th>
<th><strong>RECOMMENDATION(S)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>19. The legislation should provide that an employer must not engage in acts or practices that breach the privacy of a worker when the worker is engaged in non work-related activities without an authorisation from the regulator.</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{106} Department of Treasury and Finance (2005), above n XX, 3-3, 3-7.

\textsuperscript{107} See World Anti-Doping Agency, *World Anti-Doping Code* (2003) (WADA code) which provides for event testing and out-of-competition testing (the latter is limited to performance-enhancing substances). The federal government has agreed to be bound by the WADA code, and has indicated that Australian Olympic and non-olympic sports that wish to receive government and Australian Sports Commission funding must comply with the WADA code requirements. We have been informed that the National Rugby League (NRL) has recently adopted the code, and the Australian Football League (AFL) has indicated that it will adopt a WADA compliant Anti-Doping Code by November 2005. In addition to the WADA code, both the NRL and the AFL have sport-specific illicit drug codes. The NRL policy allows for testing for illicit drugs in the workplace during training and competition seasons. The AFL code allows for out-of-competition testing for illicit drugs.

\textsuperscript{108} Roundtable 5.
20. The regulator may authorise the employer to engage in an act or practice which affects the privacy of a worker engaged in non work-related activities, if the regulator is satisfied that:

- there are reasonable grounds for believing that the worker’s out-of-hours activity may have a direct and serious impact on the business or reputation of the employer;
- the employer’s act or practice affecting privacy cannot reasonably be undertaken while the worker is engaged in work-related activities;
- the act or practice is a proportionate response to the protection of the employer’s interests;
- the employer will ensure the act or practice is conducted appropriately;
- adequate safeguards have been put in place to minimise interference with the worker’s privacy.

OTHER PRACTICES REQUIRING AUTHORISATION

3.115 As well as requiring employers to obtain an authorisation for acts and practices which affect workers when they are not working, we recommend authorisation should be required for:

- acts or practices affecting privacy in the workers’ home;
- genetic testing;
- other prescribed practices.

PRIVACY IN WORKERS’ HOMES

3.116 A substantial percentage of workers do all or some of their work at home. The trend towards home-based work is increasing. In Victoria, the Surveillance Devices Act prohibits a person from using, installing or maintaining optical surveillance and listening devices to record private conversations or private activities to which that person is not a party, except with the consent of the person

affected.\textsuperscript{110} Many activities and conversations occurring within a worker’s home will come within the definition of private activities and conversations under the Surveillance Devices Act.\textsuperscript{111} Nevertheless, the employer can listen to or film workers in their homes if the workers consent. Some workers may feel under pressure to agree to the employer using such devices in their homes.

3.117 We have recommended the definition of work-related activities not include work which is being done in the home of a worker, except where the work involves the use of an employer’s communication system. The employer will be able to monitor the worker’s email or access to the Internet when the worker is using the employer’s communication system at home without an authorisation. However, in all other circumstances where an employer wishes to use acts or practices which affect privacy in the worker’s home, our recommendation means they will be required to obtain authorisation from the regulator.

3.118 In the commission’s view, workers are entitled to greater privacy protection in their home than in other situations. As one submission stated, ‘The employer has no business interfering with the privacy of the employee’s home’.\textsuperscript{112} Acts or practices which relate to the worker’s employment or engagement may also affect the worker’s private life. In addition, use of practices such as surveillance in a worker’s home are likely to affect the privacy of other people who live there, for example the spouse and children of the worker.

3.119 This approach is consistent with the NSW approach contained in the Workplace Surveillance Act. One important difference is that the NSW Act imposes a complete prohibition on using a work surveillance device while the employee is not at work (with the exception of computer surveillance of employer-provided equipment and resources). Non-compliance is a criminal offence.\textsuperscript{113} In comparison, we believe our proposed model offers a more flexible regulatory framework.

\textsuperscript{110} Surveillance Devices Act 1999 (Vic) s 6.

\textsuperscript{111} Under Surveillance Devices Act 1999 (Vic) s 3, a ‘private activity means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include an activity carried on outside a building. A ‘private conversation’ means a conversation carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves, but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it may be overheard by someone else.

\textsuperscript{112} Issues Paper Submission 9.

\textsuperscript{113} Workplace Surveillance Act 2005 (NSW) s 16(1), which states, ‘An employer must not carry out, or cause to be carried out, surveillance of an employee of the employer using a work surveillance device when the employee is not at work for the employer unless the surveillance is computer surveillance of the use by the employee of the equipment or resources provided by or at the expense of the employer’. Maximum penalty: 50 penalty units.
outcome in allowing employers to apply for an authorisation from the regulator. Failure to seek or comply with an authorisation is subject to a civil penalty (see Chapter 4 for the commission’s rationale on using civil penalties).

### RECOMMENDATION(S)

21. An employer must not use acts or practices which affect the privacy of a worker while they are working at home, unless the act or practice is authorised by the regulator.

22. The regulator may authorise an employer to use acts or practices which affect the privacy of workers while they are working at home if the regulator is satisfied of the matters set out in Recommendation?? :

23. An employer should not be required to seek an authorisation to monitor a worker’s email or Internet use when the worker is using the employer’s communication system, wherever the worker is situated.

### GENETIC TESTING

3.120 The commission did not discuss the issue of privacy and genetic testing in the Options Paper114 because this issue was then being considered in the joint Australian Law Reform Commission–Australian Health Ethics Committee’s (ALRC–AHEC) inquiry into the protection of human genetic information. For this reason, we go into some detail here about the issues relating to genetic testing.

3.121 A number of participants in our consultations raised concerns about genetic testing in the workplace.115 In this section, we recommend employers be required to obtain an authorisation from the regulator before undertaking genetic testing of a worker or prospective worker. In discussing this issue, we draw upon the ALRC–AHEC’s comprehensive report.116

3.122 The ALRC–AHEC report makes recommendations about the collection and use of genetic information in various contexts, including employment. In

---

114 See VLRC (September, 2004), above n XX, para 1.9.
115 See, eg, Options Paper submissions 9, 28, 31.
particular, it deals with the processes by which genetic information is obtained (this includes both genetic testing and taking a person’s family medical history), the purpose for which the information is used and the privacy protection which applies to it. In keeping with our practice-based approach, our primary concern relates to employers requiring workers to have genetic tests. This may be by doing by requiring a job applicant or worker to have a genetic test or to give the employer access to bodily samples for this purpose.

**GENETIC TESTING IN EMPLOYMENT**

3.123 The ALRC–AHEC report identifies the main reasons why employers may wish to genetically test a worker or to require the worker to give them access to the results of a genetic test:

- Genetic tests may be included in pre-employment health screening of workers to identify whether a person has a disease or other condition, or has a genetic predisposition to develop a disease or condition.119
- Genetic tests of workers can be used as part of an ongoing health surveillance program. Health surveillance designed to detect whether a person has suffered genetic damage as the result of exposure to hazardous substances, such as lead, is required in some industries.120
- Genetic tests may be used for the purposes of identification in a few industries. For example, police forces may want members to provide DNA samples to eliminate the possibility their DNA has contaminated a crime scene.121

3.124 Although use of genetic information by employers does not seem to be occurring frequently, overseas experience suggests it may become increasingly common. The ALRC–AHEC report comments that:

---

117 Genetic information may be obtained in ways which do not involve genetic testing, eg by taking a family medical history from a person. In addition, workers may provide blood and other bodily samples as part of a health examination. Employers might seek access to these samples to obtain genetic information: ALRC (2003), above n XX, vol 2, 762–4, paras 29.16–21.

118 Genetic testing includes requiring a worker to provide a bodily sample for genetic testing or to give access to bodily samples for that purpose.

119 ALRC (2003), above n XX, vol 2, 760–761; paras 29.5–29.7.

120 Ibid 761, paras 29.8–10.

121 Ibid 765, paras 29.27–30. We are informed by Victoria Police that its current policy is that collection of DNA samples for the purpose of excluding members from a crime scene can only occur if the member consents to it.
It is difficult to predict to what extent Australian employers may seek to obtain and use genetic information about job applicants or employees in the future. Australian employers already undertake a wide range of employee health assessments on a routine basis and may in future make use of genetic information as part of their pre-employment health assessment, or as part of ongoing health surveillance under occupational health and safety regulation.\(^\text{122}\)

The report also refers to the potential use of genetic tests for non-medical purposes. Associate Professor Margaret Otlowski has commented:

> Concerns about genetic screening are magnified once account is taken of future gene chip analysis and the potential for testing for a range of non-medical traits, such as aggression, alcoholism or criminality; traits that an employer would undoubtedly be keen to screen for.\(^\text{123}\)

3.125 The financial benefits for employers of screening out potentially unhealthy employees and limiting potential liability for workplace injury or disease by screening susceptible employees, may be an incentive for employers to place greater reliance on genetic testing in the future.

**REGULATION OF GENETIC TESTING OF WORKERS**

3.126 The ALRC–AHEC report identifies inadequacies in the laws which regulate collection and use of genetic information. Problems which are particularly relevant to workers include:

- no legal requirement to inform the individual about the purpose for which a sample may be used or to whom the sample may be transferred when consent is obtained to testing;\(^\text{124}\)

- limited protection against collection and genetic testing of bodily samples obtained without consent (eg by DNA testing a strand of hair);\(^\text{125}\)

- failure of the federal Privacy Act to cover genetic samples, even when they identify an individual;\(^\text{126}\)

\(^{122}\) Ibid para 29.32.

\(^{123}\) Ibid.

\(^{124}\) Ibid.

\(^{125}\) Ibid 261, para 8.2. For detailed discussion of the reasons that genetic samples are not protected see ch 8.
the exclusion of personal information contained in ‘employee records’, including genetic information from privacy protection under the federal Privacy Act;

failure of anti-discrimination laws to prohibit discrimination against a job applicant or a worker because they have a genetic pre-disposition to develop a disease or disability or on the basis of genetic characteristics which are not a disability but are considered undesirable by an employer (eg a tendency to be aggressive or shy).\(^{128}\)

3.127 Victorian laws also deal inadequately with these issues. The Victorian Equal Opportunity Act prohibits discrimination in the area of employment based on the fact that a person has an existing disability or disease but does not cover the case where a person has a genetic predisposition to develop a disability or disease, or has other genetic tendencies considered undesirable by an employer.\(^ {129}\)

3.128 The Health Records Act protects the privacy of ‘health information’, which is defined as including ‘other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or any of his or her descendants’.\(^ {130}\) However, this does not appear to cover genetic information which may be used in the future to identify traits which are not relevant to health, such as a tendency to be aggressive.\(^ {131}\)

**ALRC–AHEC RECOMMENDATIONS**

3.129 In summary, the ALRC–AHEC report makes the following key recommendations in the area of employment:

- amending discrimination laws to cover collection, use and requests for genetic information and to exclude genetic predisposition or future genetic status from the ability to perform work;\(^ {132}\)

---

128 See Otlowski (2001), above n XX.
129 *Equal Opportunity Act 1992* (Vic) s 4 has a definition of ‘impairment’. Note that this covers the presence in the body of organisms that may cause a disease, but does not cover genes which may cause a disease.
130 *Health Records Act 2001* (Vic) s 3 for the definition of personal information.
131 Otlowski (2001), above n XX, 9. Check if she says this here It is arguable that some opinions based on genetic testing could come within that part of the definition of health information that refers to an opinion about ‘the … psychological health at any time of a person’.
132 ALRC (2003), above n XX, vol ??, 783. Recommendation 30-1; 792. Recommendation 31-1; 800. Recommendation 31-3. In Victoria, this would require amending the *Equal Opportunity Act 1995* to prohibit discrimination against a person because they have a genetic predisposition to develop an
• establishing a Human Genetics Commission to make recommendations about genetic tests for screening susceptibility to particular work-related conditions;
• developing national codes for conduct of genetic screening, genetic monitoring of employees exposed to hazardous substances and assessment of workers’ compensation claims;\footnote{ALRC (2003), above n XX, vol ??, 817, Recommendation 32-2; 822, Recommendation 32-4; 841, Recommendation 33-1.}
• amending the employee records exception in the federal Privacy Act to ensure the Act protects the privacy of genetic information contained in employee records;\footnote{Ibid 841, Recommendation 33-1.}
• developing a criminal offence to cover non-consensual genetic testing.\footnote{Ibid 374, Recommendation 12-1.}

**AUTHORISATION REQUIRED FOR GENETIC TESTING**

3.130 The commission strongly supports the ALRC–AHEC recommendations. The question is whether recommendations in relation to genetic testing or use of genetic information should be included in the workplace privacy legislation. The commission recommends that, pending implementation of these recommendations at the federal level, employers who wish to genetically test workers or job applicants should seek authorisation from the regulator.

3.131 There are a number of reasons why we believe authorisation is necessary to provide an appropriate balance between workers’ privacy rights and the interests which employers may have in genetically testing workers.

3.132 Genetic testing has the potential to severely affect workers’ privacy and autonomy. Requiring a worker to undertake a test may reveal information they may not wish to know, for example, the fact that they may develop a serious disease. Genetic testing can provide information not only about the individual worker, but also about the worker’s blood relatives. The potential for genetic samples to be analysed to reveal more and more information will increase as genetic technology develops. This will enable employers to discriminate against workers who have a genetic predisposition to develop a disability or a disease, or who have other genetic characteristics. The ALRC–AHEC report found that while impairment or to manifest other physiological or psychological attributes, except where this would be permitted under other provisions of the Act. This amendment would cover discrimination on genetic grounds, whether genetic information is obtained from a test or by simply taking a medical history.
these uses of genetic information are not yet widespread, complaints about discrimination are beginning to emerge.\textsuperscript{136}

3.133 While genetic testing of workers or job applicants may be justified in certain limited situations, it is important for an employer who wishes to conduct workplace genetic testing to establish why the testing is necessary. Our recommendation limits the requirement to obtain an authorisation to situations where employers can use bodily samples to obtain genetic information about the characteristics of workers.

3.134 If an application for authorisation is made to the regulator, it can assess each case on its merits. The commission (having considered recommendations by the ALRC–AHEC) envisages that genetic testing might be authorised where:

- a worker with a genetic deficiency might be more susceptible to a particular hazard than other workers (eg workers with a genetic deficiency in the production of a particular protein are more susceptible to lung disease in dusty environments);\textsuperscript{137}

- workers are exposed to a workplace hazard such as a toxic chemical or radiation and they need to be monitored to detect the genetic effects of this exposure;\textsuperscript{138}

- genetic screening may assist in the protection of third parties;\textsuperscript{139}

- strong evidence exists of a connection between the working environment and the development of a particular condition;

- there is evidence that a condition may seriously endanger the health of an employee or the health and safety of third parties;

- there is a scientifically reliable method of screening for a condition.\textsuperscript{140}

3.135 The employer should also have to show there are no other reasonable means to eliminate or reduce the hazard which genetic testing seeks to eliminate or reduce. This is consistent with the proposed principle that acts or practices

\textsuperscript{136} Ibid.

\textsuperscript{137} ALRC (2003), above n XX, vol 2, 808, paras 32.19–21.

\textsuperscript{138} Ibid 818, para 32.54.

\textsuperscript{139} The ALRC report indicates there are restricted circumstances in which this might be reasonable. Possible examples are the testing of airline pilots or bus drivers for Huntington’s disease due to the sudden onset of irrational behaviour, or testing for Marfan Syndrome, which is difficult to diagnose but which may lead to sudden heart failure. In the vast majority of cases, the ALRC report indicates that other methods such as regular medicals would be more effective and reliable means to pick up potential issues: ibid 826, paras 32.87–89.

\textsuperscript{140} The last three requirements reflect the approach recommended in the ALRC (2003), above n XX, vol 1, 67–9.
which affect the privacy of workers should be proportionate to the purpose for which those acts and practices are being used.

3.136 Employers would also have to satisfy the regulator they had adequately informed workers about the tests and sought their views, and they had taken adequate safeguards to ensure tests are conducted appropriately.

3.137 If the broader federal protection provided by the ALRC–AHEC recommendations comes into force, the authorisation requirement may no longer be necessary.

3.138 In this context, the definition of ‘worker’ includes job applicants and other prospective workers. We have argued that the capacity of job applicants to decline breaches of privacy is illusory.\textsuperscript{141} For this reason, we believe it is appropriate to require authorisation before employers can use bodily samples to obtain genetic information about the characteristics of job applicants.

<table>
<thead>
<tr>
<th>RECOMMENDATION(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24. An employer must not conduct genetic testing of workers or prospective workers unless genetic testing is authorised by the regulator.</td>
</tr>
<tr>
<td>25. The regulator may authorise an employer to undertake genetic testing of workers if the regulator is satisfied that:</td>
</tr>
<tr>
<td>• workers have consented to being genetically tested;</td>
</tr>
<tr>
<td>• there is substantial evidence of a connection between the working environment/workplace hazard and the existence or predisposition to a condition which may be detected using genetic testing;</td>
</tr>
<tr>
<td>• the condition or predisposition which may be detected has the potential to seriously endanger the health and safety of the worker or a third party;</td>
</tr>
<tr>
<td>• there are no other reasonable means by which the hazard, which genetic testing seeks to eliminate or reduce, can be eliminated or reduced;</td>
</tr>
<tr>
<td>• there are no other reasonable means of detecting a condition;</td>
</tr>
</tbody>
</table>

\textsuperscript{141} x-ref.
26. Genetic testing means the use of samples obtained from the body of a worker, or prospective worker, for the purposes of obtaining genetic information about the worker or prospective worker.

**AUTHORISATION REQUIRED FOR OTHER PRESCRIBED PRACTICES**

3.139 We also recommend the legislation provide for regulations to be made to require authorisation of other acts or practices which have the potential to seriously affect workers’ privacy. This will ensure the legislative scheme is responsive to developments in technology and changes in societal attitudes.

27. The legislation should provide for regulations to be made requiring other acts or practices which have a serious effect on workers’ privacy to be authorised before they can be used by employers.

**FAST-TRACKING AUTHORISATIONS**

3.140 Employer groups were concerned there may be delays in obtaining authorisation for acts or practices affecting workers’ privacy. They argued it would be unnecessarily cumbersome for an employer to have to obtain authorisation to put workers under surveillance outside work, in order to discover whether they were selling property stolen from the employer. To meet this concern, the commission recommends the regulator establish a system for fast-tracking authorisations in urgent cases.
RECOMMENDATION(S)

28. The regulator should establish a system for expediting authorisation applications in urgent cases.

PROHIBITED PRACTICES

3.141 The proposed workplace privacy legislation seeks to balance employers’ interests and workers’ rights to privacy. There are some contexts in which people are entitled to have a high level of privacy protection because intrusions into their privacy have a profound effect on their human autonomy and dignity. The NSW Privacy Committee has commented that:

It is important for people to be able to preserve a distinction between their public and private worlds. The private world includes the employee’s beliefs, personal habits and conduct relating to their own body such as visiting the toilet and changing clothing. \(^{142}\)

3.142 The commission believes surveillance of workers in toilets, change rooms, lactation rooms or wash rooms is an affront to community expectations and should be prohibited. Under the Surveillance Devices Act, it is a criminal offence to install, use or maintain a listening device to listen to or record a private conversation to which the person using the device is not a party, and to install, use or maintain a video surveillance device to record visually or observe a private activity to which the person using the device is not a party. \(^{143}\) It is also an offence to publish a record of a private conversation or private activity made as the result of the use of a listening device or optical surveillance device, without the express or implied consent of each person involved in the private activity or conversation. \(^{144}\)

3.143 As para \(^{x-ref}\) explains, the Surveillance Devices Act provides limited protection to workers because conversations and activities in the workplace will often not come within the definition of ‘private conversations’ and ‘activities.’ What a worker does in a toilet or change room is likely to be regarded as a ‘private activity’. However, the Surveillance Devices Act does not prohibit surveillance in such areas if the worker consents to it. In our view, it is inappropriate for workers to be asked by an employer to consent to surveillance in such areas.

\(^{142}\) Ibid 41.
\(^{143}\) Surveillance Devices Act 1999 (Vic) ss 6–7.
\(^{144}\) Surveillance Devices Act 1999 (Vic) s 11, note exceptions in s 11(2).
3.144 A similar prohibition to the prohibition the commission proposes is contained in NSW workplace surveillance legislation. Some of the organisations and individuals we consulted also specifically referred to the unacceptability of this practice. The Victorian Trades Hall Council submission advocated:

The listing of physical locations in which breaches of privacy cannot be allowed for any reason because the nature of the breach would contravene most, if not all, of the fundamental requirements for privacy—autonomy, dignity, workers not to be treated as objects and have the capacity to form and maintain their social relationships in the workplace. Whilst not necessarily exhaustive these locations should include all relaxation/meal areas, toilets, showers, change rooms and locker rooms.

3.145 Surveillance in these private areas has a social impact that compromises the quality of life of workers in their workplaces and demeans us as a community. In this context, a prescriptive form of regulation is warranted.

3.146 Where an employer has previously used a form of surveillance in the places listed under the prohibition, it will need to devise other less invasive methods for meeting its requirements, assuming the measures are necessary at all.

### RECOMMENDATION(S)

29. An employer should be prohibited from using any device to observe, listen to, record or monitor the activities, conversations or movements of a worker in toilets, change rooms, lactation rooms or wash rooms.

### OTHER LEGISLATION

**SURVEILLANCE DEVICES ACT**

3.147 The Surveillance Devices Act already places some limits on the use of optical and audio surveillance devices and tracking devices. As we have discussed, this Act has limited relevance to workers because most conversations or activities in the workplace do not come within the definition of private conversations or

---

145 There is a prohibition on employer surveillance of employees in any change room, toilet facility or shower or other bathing facility in the workplace in *Workplace Surveillance Act 2005* (NSW) s 15.

146 Options Paper submissions 5, 28; roundtables 2, 5.

147 Options Paper Submission 28.

148 Department of Treasury and Finance (2005), above n XX, 5-11.
activities. In addition, workers who consent to surveillance are not protected. Our intention is that the Surveillance Devices Act’s provisions should no longer apply to acts or practices which are used by employers in the context of employer–worker relationships. In other words, the workplace privacy legislation will comprehensively regulate practices that affect workplace privacy. The Surveillance Devices Act should be amended to make this clear.

**LAW ENFORCEMENT**

3.148 As is currently the case under the Surveillance Devices Act, the workplace privacy legislation is not intended to affect the powers which members of Victoria Police and other state and federal bodies exercise for law enforcement purposes, and which are regulated by other legislative controls. For example, the proposed legislation is not intended to cover police video surveillance of a worker to detect criminal activity.

3.149 There may be some situations in which the act or practice affecting a worker is being done by an employer which is also a law enforcement agency. Victoria Police are the obvious example. On the one hand, police could be seen as workers with rights to privacy protection. While police occupy a special position in society, they are entitled to protection of their human rights along with every other member of the community. On the other hand, they are law enforcement officers. In some cases these roles may overlap. For example, a decision may be made to place a police officer under surveillance because it is suspected the officer is involved in criminal activity.

3.150 The Police Regulation Act 1958 deals with the employment and disciplining of police, the investigation of disciplinary matters and associated powers. It establishes an Office of Police Integrity, the Director of which is to ensure the maintenance of the highest professional standards and ensure corruption and serious misconduct is detected, investigated and prevented.

3.151 Issues which are particularly relevant to police should be dealt with under specific legislation rather than under the workplace privacy legislation proposed in this report. The Victorian Privacy Commissioner has responsibility for, and

---

149 See *Surveillance Devices Act 1992 (Vic)* s 3 for definition of law enforcement officer.
150 Cf *Surveillance Devices Act 1999 (Vic)* ss 5, 9, 10, 12, pt 4.
151 Police officers occupy a different position than that expected within a standard employer–employee relationship. See *Police Regulation Act 1958 (Vic)* s 11, which states, ‘Every constable shall have such powers and privileges and be liable to all such duties as any constable duly appointed now has or hereafter may have either by the common law or by virtue of an Act of Parliament now or hereafter to be in force in Victoria, and any member of the police force of a higher rank than a constable shall have all the powers and privileges of constable whether conferred by this Act or otherwise’.
considerable experience in, considering the balance to be struck between privacy protection and other public policy concerns. We would expect the government to consult with the Privacy Commissioner about how privacy issues relevant to the police should be dealt with.\footnote{152}{The commission is aware that amendments to the Police Regulation Act are under consideration by the Victorian Government.}

**OTHER LEGISLATION**

3.152 Some acts or practices regulated under our proposed legislation may be expressly permitted under other legislation. The commission has not attempted to identify all the statutory provisions which affect practices considered in this report. If the government establishes the regulatory regime we recommend, it should consult government agencies and statutory authorities to identify such provisions and determine whether they should be retained. For this reason, the draft Bill in Appendix 2 does not contain statutory exceptions to deal with powers contained in other legislation, but it may be necessary to include such exceptions.

<table>
<thead>
<tr>
<th>RECOMMENDATION(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30. Acts or practices of employers which involve installation, use or maintenance of surveillance devices, in relation to their workers should be regulated by the Workplace Privacy Act. The Surveillance Devices Act should be amended accordingly.</td>
</tr>
<tr>
<td>31. The Department of Justice should consult with government agencies and statutory entities to determine whether statutory provisions in other legislation which affect workplace privacy should be repealed or retained.</td>
</tr>
</tbody>
</table>