Victorian
Law Reform
Commission

# Workplace Privacy

## Options Paper

Victorian Law Reform Commission

GPO Box 4637
Melbourne Victoria 3001
Australia
DX 144 Melbourne, Vic

Level 10
10-16 Queen Street
Melbourne Victoria 3000
Australia

Telephone +61 3 8619 8619
Facsimile +61 3 8619 8600
TTY 1300 666 557
1300 666 555 (within Victoria)
law.reform@lawreform.vic.gov.au
www.lawreform.vic.gov.au

## CALL FOR SUBMISSIONS

The Victorian Law Reform Commission invites your comments on this Options Paper and seeks your responses to the recommendations and questions that are raised. If you wish to make a submission to us on this reference, you can do so by mail, email, phone, fax or in person. If your submission is in writing, there is no particular form or format you need to follow. If you prefer to make a submission by phone or in person, contact the Commission and ask to be put through to one of the researchers working on the Privacy reference. You can send your written submissions by post, or by email to <law.reform@lawreform.vic.gov.au>.

If you need any assistance with preparing a submission, please contact the Commission. If you need an interpreter, please contact the Commission.

If you would like your submission to be confidential, please indicate this clearly when making the submission. If you do not wish your submission to be quoted, or sourced to you in a Commission publication, please let us know. Unless you have requested confidentiality, submissions are public documents, and may be accessed by any member of the public.

## DEADLINE FOR SUBMISSIONS: 30 NOVEMBER 2004

Published by the Victorian Law Reform Commission.

The Victorian Law Reform Commission was established under the *Victorian Law Reform Commission Act 2000* as a central agency for developing law reform in Victoria.

This Options paper reflects the law as at 30 July 2004.



The publications of the Victorian Law Reform Commission follow the Melbourne University Law Review Association Inc *Australian Guide to Legal Citations* (2nd ed, 2002).

Designed by Andrew Hogg Design.

Developed by Linton (Aust) Pty Ltd.

National Library of Australia

Cataloguing-in-Publication

Workplace privacy: options paper.

Bibliography.

ISBN 0 9751497 4 1.

1. Privacy, Right of – Victoria. 2. Employee rights – Victoria. 3. Confidential communications – Victoria. 4. Electronic monitoring in the workplace – Victoria. I. Victorian Law Reform Commission.

344.9450101

# Contents

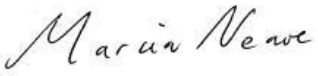
# Preface

The publication of this Options Paper marks the second part of the first stage of the Victorian Law Reform Commission's reference on privacy, which focuses on privacy within the workplace. The Paper is intended to stimulate discussion about possible regulatory reform to the current law, and provide the basis for the Commission's final consultations on law reform in the area of workplace privacy. The Options Paper examines the constitutional parameters of the reference, proposes a conceptual framework for workplace privacy, describes the practices that it covers and examines the gaps in protection identified through general research and stakeholder consultations. The Options Paper proposes possible options for the regulatory reform of workplace privacy. The Paper asks a series of questions on which the Commission seeks comment from employers, workers and members of the public. After a period of consultation, the Commission will then prepare its Final Report containing recommendations to the Attorney-General.

Production of the Options Paper was a team effort. Research and Policy Officers Susan Coleman and Priya SaratChandran were the authors of the Paper. They should be congratulated for their hard work and intellectual rigour. Alison Hetherington edited the Paper. Julie Bransden prepared the Bibliography and chased up many obscure references. Kathy Karlevski prepared the Paper for publication and Lorraine Pitman was involved in the production process. Matthew Carroll and Padma Raman provided valuable strategic advice throughout various stages of the Paper. Members of the Workplace Privacy Division, AIRC Vice-President Iain Ross and Professor Sam Ricketson oversaw the work on the Paper and made many contributions to its drafting.

In preparing the Paper, the authors were greatly assisted by the two constitutional consultants engaged by the Commission, Ms Amelia Simpson, a member of the Advisory Committee on this reference, and Mr James Stellios. I am grateful to all our consultants for their time and input, but particularly to a number of our technical consultants including, Mr Nick Carter, Mr Arthur Crook, Adjunct Professor Olaf Drummer, Dr Ian Freckelton, and Mr Mike Thompson who advised on technical issues and reviewed drafts of Chapter 2. I also wish to thank Mr Chris Maxwell QC and Mr Peter Wischusen for their expertise on comparative jurisdictions, as well as Mr Brian Corney, Mr Eamonn Moran QC and Mr Nigel Waters in advising us on legislative issues. I would also like to acknowledge the assistance of Mr Ben Rice of the Equal Opportunity Commission of Victoria for his provision of research sources. Special thanks as well to Dr Breen Creighton, who at very short notice, provided us

with the benefit of his employment law expertise. I also thank the Advisory Committee for their time and support and the representatives of employers and employees who participated in our consultations.



Marcia Neave
Chairperson

# Contributors

| | |
|---|---|
| **Authors** | Susan Coleman |
| | Priya SaratChandran |
| **Editor** | Alison Hetherington |

**Victorian Law Reform Commission**

| | |
|---|---|
| *Chairperson* | Professor Marcia Neave AO* |
| *Commissioner* | Judith Peirce |
| *Part-time Commissioners* | Paris Aristotle AM |
| | Her Honour Judge Jennifer Coate |
| | The Honourable Justice David Harper |
| | Professor Felicity Hampel SC |
| | Professor Sam Ricketson* |
| | Dr Iain Ross* |
| *Chief Executive Officer* | Padma Raman |
| *Operations Manager* | Kathy Karlevski |
| *Policy and Research Team Leaders* | Angela Langan |
| | Mary Polis |
| *Policy and Research Officers* | Liana Buchanan |
| | Susan Coleman |
| | Nicky Friedman |
| | Hilary Little |
| | Siobhan McCann |
| | Victoria Moore |
| | Priya SaratChandran |
| *Communications Officer* | Alison Hetherington |
| *Project Officer* | Simone Marrocco |
| *Librarian* | Julie Bransden |
| *Administrative Officers* | Lorraine Pitman |
| | Nadia Vitellone |
| | Jenny Wright |

* Privacy Division, constituted under Section 13 of the *Victorian Law Reform Commission Act 2000.*

# Terms of Reference

In light of the widespread use of surveillance and other privacy-invasive technologies in workplaces and places of public resort, and the potential benefits and risks posed by these technologies, the Victorian Law Reform Commission will inquire into and report progressively upon:

(a) whether legislative or other reforms should be made to ensure that workers' privacy, including that of employees, independent contractors, outworkers and volunteers, is appropriately protected in Victoria. In the course of this inquiry, the Commission should consider activities such as:

- surveillance and monitoring of workers' communications;
- surveillance of workers by current and emerging technologies, including the use of video and audio devices on the employers' premises or in other places;
- physical and psychological testing of workers, including drug and alcohol testing, medical testing and honesty testing;
- searching of workers and their possessions; and
- collecting, using or disclosing personal information in workers' records.

(b) whether legislative or other measures are necessary to ensure that there is appropriate control of surveillance, including current and emerging methods of surveillance, and the publication of photographs without the subject's consent. As part of this examination, the Commission should consider whether any regulatory models proposed by the Commission in relation to surveillance of workers could be applied in other surveillance contexts, such as surveillance in places of public resort, to provide for a uniform approach to the regulation of surveillance.

In undertaking this reference, the Commission should have regard to:

- the interests of employers and other users of surveillance, including their interest in protecting property and assets, complying with laws and regulations, ensuring productivity and providing safe and secure places;
- the protection of the privacy, autonomy and dignity of workers and other individuals;
- the interaction between state and Commonwealth laws, and the jurisdictional limits imposed on the Victorian Parliament; and
- the desirability of building on the work of other law reform bodies.

# Abbreviations

| | |
|---|---|
| **AHEC** | Australian Health Ethics Committee |
| **AIRC** | Australian Industrial Relations Commission |
| **ALRC** | Australian Law Reform Commission |
| **AMA** | Australian Medical Association |
| **APS** | Australian Psychological Society |
| **CCTV** | closed-circuit television |
| **EOA** | *Equal Opportunity Act 1995* (Vic) |
| **EOCV** | Equal Opportunity Commission of Victoria |
| **GPS** | Global Positioning System |
| **HRA** | *Health Records Act 2001* (Vic) |
| **IPA** | *Information Privacy Act 2000* (Vic) |
| **n** | footnote |
| **NATA** | National Association of Testing Authorities |
| **NHMRC** | National Health and Medical Research Council |
| **OHS** | occupational health and safety |
| **para** | paragraph |
| **s** | section (ss plural) |
| **SDA** | *Surveillance Devices Act 1999* (Vic) |
| **SMS** | short message service |
| **TIA** | *Telecommunications (Interception) Act 1979* (Cth) |
| **VCAT** | Victorian Civil and Administrative Tribunal |
| **Vic** | Victoria |
| **VLRC** | Victorian Law Reform Commission |
| **VTA** | Victorian Transport Authority |
| **WRA** | *Workplace Relations Act 1996* (Cth) |

# Executive Summary

## PURPOSE AND SCOPE OF THIS OPTIONS PAPER

This Options Paper is the next phase in the Commission's reference on workplace privacy.[1] The terms of reference require the Commission to look into whether workers' privacy in Victoria is adequately protected.

The Commission has examined the current legislative regime and found there are significant gaps in workers' privacy protection in Victoria,[2] particularly in relation to surveillance, monitoring and testing practices used by employers. For this reason, the focus of this Paper is on these three key areas.

The purpose of this Paper is to:

- reflect the attitudes of employers and workers to workplace privacy issues involving surveillance, monitoring and testing;
- critically examine the perspectives of employers and workers to determine whether there is a case for law reform;
- put forward options for law reform in relation to surveillance, monitoring and testing practices. The aim of each option is to provide a mechanism to balance the interests of employers with the privacy interests of workers; and
- seek comments from employers, workers and other interested parties on the proposed options.

As federal legislation already exists on information privacy, this has posed certain constitutional restrictions on Victoria's ability to legislate in this area. To counter this, we have adopted a 'practice-based' approach that looks at the practices of surveillance, testing and monitoring and the impact on worker's privacy, prior to information being created. We also place 'privacy' within a human rights conceptual framework, applicable not only in the workplace, but in all other areas of public life. This does not mean privacy is an absolute entitlement, but rather that it is subject to the balancing of other social values and interests.

1 See the terms of reference on page viii.

2 See Victorian Law Reform Commission, *Workplace Privacy* Issues Paper (2002) (hereafter Issues Paper).

## TECHNOLOGIES AND PRACTICES

Technology is becoming more sophisticated, while at the same time becoming cheaper and more accessible to employers. In Chapter 2 we describe the key surveillance, monitoring and testing technologies and practices that are, or are likely to become, commonly used in the workplace. These include:

- video surveillance;
- telephone monitoring;
- use of tracking devices;
- use of biometric technologies;
- email and Internet monitoring;
- medical testing;
- psychological testing; and
- drug and alcohol testing.

In Chapter 2 we also briefly examine the way in which these practices are regulated. We review the potential privacy protection gaps under the *Surveillance Devices Act 1999* and the *Telecommunications (Interception) Act 1979* (Cth) in the regulation of workplace surveillance and monitoring practices, including the use of biometric technologies. We also review the regulation of workplace medical, psychological, drug and alcohol testing. In the case of testing, apart from the *Health Records Act 2001* there is little, if any, regulation which protects workers' privacy.

## GAPS IN PROTECTION

In Chapter 3 the Commission examines the attitudes of employers and workers to workplace surveillance, monitoring and testing practices. We also explain how these practices can affect third parties in the workplace (such as visitors).

Chapter 3 reflects on information obtained from our consultations with employers, employer associations, unions and experts in the practices and technologies covered in this Paper. It also includes information contained in submissions to the Commission's Issues Paper.

Consultations and submissions revealed that employers have embraced surveillance and monitoring technologies and testing practices for a variety of reasons. These include protection of property, maintenance of security, selecting and measuring worker performance, reducing the risk of legal liability and evidence gathering. At the same time, workers are concerned about the potential of certain practices to compromise their autonomy and dignity in the workplace and to negatively affect the relationship of trust between employers and employees. Added to this are the practical

difficulties surrounding worker consent due to power imbalances between employers and workers, the lack of transparency as to how and why practices are being used, the inaccuracy of certain practices in assessing suitability for work, and the potential for discrimination resulting from the use of such practices.

In analysing these issues it is clear to the Commission that the status quo is not adequate in either protecting workers' privacy or properly addressing employer concerns. The Commission believes that reform of the law in this area is essential to provide the necessary regulatory guidance to enable the complex interests of employers and workers to be appropriately balanced.

## OPTIONS FOR REFORM

In Chapter 4 the Commission proposes two broad options for reform. The Commission's aim is not to prohibit employers from using surveillance, monitoring and testing in the workplace. Its aim is to propose alternative ways in which the interests of employers and workers can be appropriately balanced to address the issues outlined in Chapter 3.

In considering options for reform, the Commission has three goals:

- to ensure minimum standards of privacy protection for workers without unduly limiting the ability of employers to run their businesses;
- to protect workers' privacy in a way that is sufficiently flexible to accommodate the needs of different workplaces;
- to put in place mechanisms that ensure compliance with the selected regime.

### OPTION 1

Option 1 proposes a separate Act that requires employers to seek authorisation in advance before conducting any (or some) surveillance, monitoring or testing. The core protection in the Act would be designed to ensure that the privacy of workers can only be restricted where some or all of those practices are appropriately authorised.

The key feature of the Act would be to require employers to seek written authorisation from a regulator before conducting some or all types of overt and covert surveillance, monitoring or testing in the workplace. The Act could allow employer associations to apply for authorisations on behalf of their members where practices are commonly used throughout a particular industry sector (such as video surveillance in the retail sector).

Other features of this option could include:

- a process for notifying workers that an application for authorisation has been submitted to the regulator (with the exception of certain covert practice applications);
- a process for workers to be properly consulted about the application (either by the regulator or the employer);
- powers for the regulator to conciliate or hear disputes about the application between the employer and workers;
- a complaints-based mechanism;
- powers for the regulator to conciliate or investigate worker complaints, and to enforce the Act and authorisation conditions by having the ability to audit employers and issue compliance notices;
- an educative role to be fulfilled by the regulator; and
- removal of workplace surveillance issues from the *Surveillance Devices Act 1999*.

## OPTION 2

Option 2 proposes a separate Act containing principles which employers would be required to follow when implementing workplace surveillance, monitoring or testing.

Other features of this option could include:

- a code or codes produced by the regulator (or an equivalent, developed by industry and approved by the regulator) to provide practical details on how employers can comply with the principles in relation to particular practices—the codes would not be binding, but compliance with a code could be used by employers to defend themselves against worker complaints;
- a complaints-based mechanism with powers for the regulator to conciliate or investigate complaints about breaches of the principles;
- powers for the regulator to issue compliance notices for serious breaches of the Act;
- an educative role to be fulfilled by the regulator; and
- removal of workplace surveillance issues from the *Surveillance Devices Act 1999*.

## THE OPTIONS COMPARED

Both the options would achieve the three goals described above—minimum standards, flexibility and enforcement—but in different ways and to different degrees. Option 1 would require the authorisation of all or some workplace surveillance, monitoring and

testing practices before they are implemented, whereas Option 2 would require employers to follow certain principles when instituting and applying such practices and is reliant on a complaints-trigger.

Option 1 would have some resource implications for the government and, depending on the extent and use of practices, for employers. But it would provide greater certainty about acceptable and unacceptable practices for employers and workers than Option 2. It also has a more stringent enforcement regime than Option 2. Option 2 would put more direct responsibility on employers and may require less resources.

The Commission is seeking submissions and comments on the options. We are interested to hear views about whether part or all of an option is preferred and about any practical issues that may arise in relation to these options.

# Questions

## OPTION 1

1. Should employers be required to seek authorisation from a regulator before conducting workplace surveillance, monitoring and testing? If so, what issues should be considered by the regulator in determining whether to authorise the use of these practices?

2. Are there any practical difficulties with the concept of industry-wide authorisations?

3. Are there any surveillance, monitoring or testing practices which should be permitted without authorisation? If so, which ones and why?

4. Should overt and covert practices be treated differently? If so, why?

5. Should there be a mechanism to ensure proper consultation or communication with workers during the authorisation process? What is the best way to do this?

6. How can such a procedure be made effective, given the imbalance of power that may exist between an employer and workers?

7. Would it be more appropriate for a court to assess authorisation applications than a regulator?

8. Is the proposed test to be used by the regulator that a practice is 'reasonable in the circumstances' an appropriate one?

9. What is the preferred method of handling complaints—conciliation or direct investigation by the regulator, or some element of both?

10. In your experience of other jurisdictions where the regulator has an inspectorate (such as OHS), how effective is the inspectorate model?

11. What level and kinds of penalties should there be for breaches of the Act?

12. Is this enforcement regime appropriate? Are there any other mechanisms for enforcement that should be considered?

13. Should there be some lead time before the authorisation process applies?

## OPTION 2

14. If legislation were enacted to introduce principles to govern workplace surveillance, monitoring and testing, what should those principles be?

15. If codes are used to provide detail on complying with the general principles, should the codes be mandatory? Should they be used in some other way?

16. Has this model been effective in other jurisdictions?

17. Have the advantages and disadvantages of Options 1 and 2 been adequately identified?

18. Do you prefer the option requiring 'authorisation in advance' or the option incorporating general principles? Explain your preference.

19. Would you prefer an option that combines aspects of each option? If so, which parts of each? Would you prefer a different option?

# Chapter 1
# Introduction

## SCOPE OF THE REFERENCE ON WORKERS' PRIVACY

1.1 In March 2002, the Victorian Attorney-General asked the Commission to examine two major issues of public concern in relation to privacy: workers' privacy and privacy in public places. The focus of the current phase of our inquiry is on workers' privacy. This includes an examination of activities such as worker surveillance and monitoring, physical and psychological testing of workers, searching of workers and their belongings, and the handling of workers' personal information. In the next phase of our project we will investigate surveillance in public places.[3]

## PURPOSE AND SCOPE OF THIS OPTIONS PAPER

1.2 In the past, if an employer wanted to monitor a worker's performance or behaviour this would involve some form of personal observation. Those days are gone. Almost daily, newspapers report on the erosion of privacy within the workplace. As rapid developments in technology and medical science become increasingly invasive and available, serious concerns are being expressed about the privacy rights of workers. The seemingly unprecedented ability to observe, monitor and test individuals is not only of concern to workers but to the wider community. Concern about these issues has prompted the New South Wales Government to review workplace video surveillance legislation. It now proposes to broaden the scope of that legislation to regulate other forms of surveillance, including workplace email and Internet monitoring.[4]

---

3 See the terms of reference on page viii.

4 The New South Wales Government has released an exposure draft of the Workplace Surveillance Bill 2004. According to the Explanatory Note to the Bill, the objects of the Bill are to: (a) prohibit surveillance by employers of their employees at work, except where the surveillance is notified to employees or surveillance is carried out under the authority of a covert surveillance authority issued by a magistrate for the purpose of establishing whether or not an employee is involved in any

1.3 As part of its initial review, the Commission examined Victorian law relating to workplace privacy issues.[5] That examination revealed that although historically the focus of privacy legislation has been the creation, use and handling of personal information about individuals—'information privacy'—significant gaps exist in workers' privacy protection before any information is created, that is, in relation to the actual practices of surveillance, monitoring and testing in the workplace.[6] Our consultations with employer representatives also revealed a level of uncertainty about what employers can and cannot do in relation to such practices. For these reasons, the focus of this Options Paper is on issues surrounding the *processes* of surveillance (including the use of biometric technologies), monitoring and testing by employers. We consider how the use of these practices in the workplace might be regulated, balancing the interests of employers in running their businesses with the privacy rights of workers.

1.4 Throughout the Options Paper we use the term 'workers' instead of 'employees'. We do this for two reasons. The first is that our terms of reference require us to examine the privacy of 'workers' which is not limited to those defined as employees, but can extend to groups not usually considered employees such as volunteers, independent contractors and outworkers. We also include job applicants under the term 'worker', as they are particularly affected by practices such as medical and psychological testing.

1.5 The second reason stems from the way in which we have chosen to conceptualise 'privacy'. Although the reference deals specifically with workplace privacy, we do not view privacy as a workplace-specific entitlement. For this reason we do not consider that any proposed regulation of workplace privacy needs to follow the regulatory structure of other labour rights. Instead, we conceptualise privacy within a human rights framework[7] applicable not only in the

---

unlawful activity at work; (b) to restrict and regulate the blocking by employers of emails and Internet access of employees at work; (c) to provide for the issue of covert surveillance authorities by magistrates and to regulate the carrying out of surveillance under a covert surveillance authority and the storage of covert surveillance records; and (d) to restrict the use and disclosure of covert surveillance records. The Bill applies to camera surveillance, computer surveillance and tracking surveillance (surveillance of the location or movement of an employee). The Bill is intended to replace the existing *Workplace Video Surveillance Act 1998* (NSW) which applies only to video (ie camera) surveillance.

5 See the Issues Paper, Chapter 4.

6 Ibid paras 4.79–83, 4.105–111.

7 For a detailed discussion of privacy within a human rights framework see Kate Foord, *Defining Privacy* (2002) (hereafter Occasional Paper) pp 20–28 and Issues Paper paras 2.1–2.38.

workplace, but to all other regulated areas of public life.[8] Conceiving of privacy within a human rights framework is an approach mirrored in Article 12 of the United Nations Universal Declaration of Human Rights,[9] in Article 8 of the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms,[10] as well as in the Victorian Government's recently released Attorney-General's Justice Statement.[11]

1.6 Although there are privacy issues peculiar to the workplace (which are described in this Paper), as an entitlement placed within a human rights framework, privacy should properly apply to all areas of public life, though this does not necessarily mean it is an absolute entitlement. This approach is similar to that reflected in federal and state anti-discrimination legislation which, while placed within a human rights framework,[12] does not provide for absolute rights, but rights that are subject to certain exceptions/exemptions.[13] Being human rights-

8 The *Equal Opportunity Act 1995* covers areas of public life such as employment, employment-related areas, education, provision of goods and services, accommodation, clubs and club members, sport and local government.

9 United Nations, *Universal Declaration of Human Rights*, adopted and proclaimed by General Assembly resolution 217 A (111) of 10 December 1948 in Article 12 states, 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks'.

10 Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11* in Article 8, which states '(1) Everyone has the right to respect his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, or the protection of health or morals, or for the protection of the rights and freedoms of others'.

11 Department of Justice, *New Directions for the Victorian Justice System 2004–2014: Attorney-General's Justice Statement* (2004) 53 which under '4.2 protecting human rights' lists 'privacy' as part of 'Victorians' enjoyment of their human rights'.

12 See for example *Disability Discrimination Act 1992* (Cth) s 12; *Race Discrimination Act 1975* (Cth) s 3 and Schedule; *Sex Discrimination Act 1984* (Cth) s 4 and Schedule; the Victorian Attorney-Generals' Justice Statement (Justice Statement, n 11) refers to the *Equal Opportunity Act 1995* under 4.2 'Protecting Human Rights' and under 4.2.2 describes 'human rights protection in Victoria' as 'focused on protecting people from discrimination', 56. Note that the United Nations Universal Declaration of Human Rights (Universal Declaration, n 9) also refers specifically to discrimination in Article 7 which states, 'All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination'.

13 Exceptions exist with respect to all the public grounds listed in these Acts with general exemptions available under each Act. See for example *Disability Discrimination Act 1992* (Cth) div 5; *Race*

based, the objectives of anti-discrimination legislation are benevolent in nature.[14] Similarly, we see privacy as benevolent in nature. This underpins our broad approach to defining terms such as 'worker', 'employer' and 'workplace'.

1.7 In accordance with this approach, we use the term 'worker' to describe employees as well as those persons whose privacy may be infringed in their capacity as 'workers'. The term 'employer' is usually used to describe a person or organisation that engages another person to perform work or unpaid services.[15] In this Paper we use the term 'employer' broadly to describe these situations, as well as situations where a contract worker is engaged by an organisation and where a person has not yet been employed.

1.8 Similarly, we take a broad view of the term 'workplace'. The term 'workplace' will be used to mean 'any place, whether or not in a building or structure, where employees or self-employed persons work'.[16] This is because workplaces are extremely varied and our terms of reference require us to examine surveillance by employers on their premises or in other places.[17] However, our definition of 'voluntary' work is not taken to include unpaid domestic work, predominantly performed by women, which forms the most significant proportion of unpaid labour in Australia.[18] Although we recognise the importance of this work, we do not consider the issues raised by the Workplace Privacy reference to be directly relevant to it.

1.9 Although we consider the use of emerging technologies in this Paper, we do not address issues of privacy and genetic testing of workers. These issues have been covered comprehensively by the Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) in their report *Essentially Yours:*

---

*Discrimination Act 1975* (Cth) s 18D; *Sex Discrimination Act 1984* (Cth) div 4; *Equal Opportunity Act 1995* s 12, pt 4 (a mixture of exemptions and exceptions).

14 See the objectives in the *Equal Opportunity Act 1995* s 3 which states, 'The objectives of this Act are: (a) to promote recognition and acceptance of everyone's right to equality of opportunity; (b) to eliminate, as far as possible, discrimination against people by prohibiting discrimination on the basis of various attributes; (c) to eliminate, as far as possible, sexual harassment; (d) to provide redress for people who have been discriminated against or sexually harassed. The 'objectives' suggest a protective approach towards workers in 'as far as possible'.

15 Peter Nygh and Peter Butt (ed) *Butterworths Australian Legal Dictionary* (1997) 414.

16 This is the definition of 'workplace' used in s 4 of the *Occupational Health and Safety Act 1985*.

17 See the terms of reference on page viii.

18 Breen Creighton and Andrew Stewart, *Labour Law: An Introduction* (3rd ed) (2000) 2.

*the Protection of Human Genetic Information in Australia.*[19] This report recommended employers should not collect and use genetic information except in rare circumstances.[20] The Commission supports the ALRC and AHEC's recommendations on this issue.

1.10 The issue of searching of workers and their belongings will be addressed in the final stage of the reference.

## WORK TO DATE ON THE REFERENCE

1.11 As a means of engaging with interested individuals and organisations, the Commission published the *Workplace Privacy Issues Paper* in October 2002. The Issues Paper discussed the meaning of privacy based on notions of autonomy and dignity. It examined the extent to which current privacy and workplace relations laws protect workers' privacy and canvassed possible approaches to reform. The Commission received 34 submissions, mostly from organisations and representative bodies, in response to the Issues Paper.[21] At around the same time, the Commission published an Occasional Paper, *Defining Privacy*. The Occasional Paper provided a rigorous discussion and analysis of approaches to defining privacy which formed the basis of the definition of privacy used in the Issues Paper.[22]

## CONSULTATIONS

1.12 Submissions to the Issues Paper provided the Commission with valuable information concerning privacy issues in Victorian workplaces and attitudes towards regulation. To investigate the key areas of surveillance, monitoring and testing, we met with various employer associations, employers and unions. These

19 Australian Law Reform Commission, *Essentially Yours: the Protection of Human Genetic Information in Australia, Volume 2* Report 96 (2003) (hereafter the ALRC Report).

20 See ibid, particularly Part H and Recommendations 30–1, 34–2. The ALRC Report recommends that as a general matter, employers should not collect or use genetic information in relation to job applicants or employees. However, the ALRC Report acknowledges there may be rare circumstances where such action is necessary to protect the health and safety of workers or third parties and this should be permitted if the action complies with stringent privacy, anti-discrimination and occupational health and safety safeguards. The recommended occupational health and safety safeguards include stringent standards developed by a new body called the Human Genetics Commission of Australia and the National Occupational Health and Safety Commission.

21 A list of the submissions is shown in Appendix 1.

22 See the discussion in paras 1.14–1.19 on 'defining privacy'.

meetings provided a representative sample of the types of industries undertaking surveillance, monitoring and testing of workers.[23] However, we recognise our consultation process has not covered every type of employer and worker.

1.13 In addition to employer and worker representatives, we consulted individuals and organisations with relevant technical knowledge. These consultations provided us with information about how surveillance and monitoring technologies work in practice. They also informed our understanding of how medical, drug and alcohol, and psychological tests are undertaken in the workplace and what they measure.

## OUR APPROACH TO THE REFERENCE

### DEFINING PRIVACY

1.14 In the Issues Paper and the Occasional Paper, the Commission proposed privacy be defined as:

- the right not to be turned into an object or statistic; that is, the right of people not to be treated as if they are things; and
- the right to establish and develop relationships with other human beings.[24]

The foundations of this definition are the concepts of human autonomy and dignity and the protection of privacy as a social value rather than just as an individual right. Under this approach, the right to privacy is not an absolute right and is balanced alongside other social values, such as the provision of a safe workplace and the employer's interest in having workers perform the work they are engaged to do. In the Issues Paper, we highlighted the importance of context in assessing whether a particular practice is privacy invasive or not.[25] We recognised that in the employment context, the privacy rights of workers need to be balanced against the interests of employers in running their businesses.[26] The issue of balancing interests is explored further in Chapters 3 and 4.

23 A list of the consultations is shown in Appendix 2. A list of organisations we met with is shown in Appendix 3.

24 See Issues Paper, Chapter 2.

25 Ibid paras 2.52–3.

26 Ibid.

1.15 Several submissions commented on the Commission's proposed definition of privacy.[27] Generally, these submissions supported some kind of rights-based or interest-based approach underpinned by notions of autonomy and dignity.[28] However, some submissions were critical of a rights-based approach. For example, the Australian Bankers' Association commented that following a 'privacy-right path' would be in direct conflict with the soft touch approach of the *Privacy Act 1988* which balances the protection of individuals' personal information with modern business activity.[29]

1.16 Submissions supportive of a rights-based approach generally indicated that the proposed definition of privacy did not go far towards providing a basis for regulatory reform. The Equal Opportunity Commission of Victoria said in its submission:

> …there is a risk that this working definition of privacy will not be practical for the development of a framework for a workplace privacy regime. Even after exposure to this definition of privacy, it is possible that employers and employees will not gain any practical understanding of what their rights and responsibilities are in relation to privacy in the workplace.[30]

1.17 The Australian Privacy Foundation agreed privacy should be a right and a social value, but argued the proposed definition may not be sustainable for recommending law reform. Rather, the Foundation suggested a definition of privacy should recognise the importance of a person's expectations and wishes about the boundaries between their public and private lives and:

> …determining what is an invasion of privacy depends on the context. It is unlikely that any definition will suffice and the real task becomes to determine which aspects of the context are significant.[31]

1.18 The difficulty in defining privacy as a legal principle was recently highlighted by a case in the United Kingdom.[32] In a judgment in that case, Lord

---

27 For example, Submissions 14, 15, 16, 22, 23, 24, 25, 26, 28, 29, 31.

28 For example, Submissions 14, 15, 22, 25, 29.

29 Submission 26.

30 Submission 22.

31 Submission 15.

32 See *Wainwright and Another v Home Office* [2003] UKHL 53 (16 October 2003). The case concerned whether two individuals who had been inappropriately strip searched by prison authorities had a right to sue for breach of privacy. The House of Lords declined to recognise a general tort of invasion of privacy as part of English law. Note that in *Campbell v MGN Limited* [2004] UKHL 22

Hoffman indicated there is a difference between identifying privacy as a value which underlies the law and privacy as a value in itself.[33] He indicated there are certain underlying values which direct the development of the law and which do not need to be defined as separate legal principles. He gave as an example freedom of speech, which is not itself a separate legal principle but which underpins the law of libel.[34] Similarly, he considered that a high level privacy principle was not required to comply with a European convention that provides that everyone's private life should be respected.[35] In New Zealand, a recent case found there is protection for an interference with privacy in respect of publication of private facts.[36] The majority of judges in that case did not offer a comprehensive definition of privacy, but examined the concept of a 'reasonable expectation of privacy'. One of the majority judges said:

---

(6 May 2004), the House of Lords upheld model Naomi Campbell's claim for invasion of privacy, based on misuse of private information. The claim resulted from the publication of an article by the *Daily Mirror* about Ms Campbell's battle with drug addiction and included a photograph of Ms Campbell leaving a meeting of Narcotics Anonymous. The key issue in the case was whether the public interest in favour of publication outweighed the public interest in protecting Ms Campbell's rights to confidentiality. The House of Lords found in favour of Ms Campbell by a majority of three to two. The House of Lords reached their decision by effectively extending the existing action for breach of confidence. They did not attempt to define the concept of privacy.

33 *Wainwright and Another v Home Office* [2003] UKHL 53 (16 October 2003) para 31 (Lord Hoffman).

34 *Wainwright and Another v Home Office* [2003] UKHL 53 (16 October 2003) para 31 (Lord Hoffman).

35 *Wainwright and Another v Home Office* [2003] UKHL 53 (16 October 2003) para 32 (Lord Hoffman). Lord Hoffman was referring to compliance with Article 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms*, which is described at n 10. The principles contained in Article 8 of the Convention have since been enacted into English law through the *Human Rights Act 1998* (UK). Lord Hoffman considered that the European Court of Human Rights would only be concerned with whether English law provides an adequate remedy in a specific case where it considers there has been an invasion of privacy contrary to Article 8(1) which is not justifiable under Article 8(2).

36 *Hosking & Hosking v Simon Runting & Anor* [2004] NZCA 34 (25 March 2004). The case involved the dismissal of an appeal by a New Zealand media personality, Mike Hosking, and his estranged wife. Mr and Mrs Hosking failed to obtain an injunction to prevent publication of photographs of their twin baby daughters which had been taken in a public street. However, even though the court did not find in favour of the Hoskings, the majority of the court decided there is protection for an interference with privacy in respect of the publication of private facts. Gault P (in a joint judgment with Blanchard J) expressed the fundamental requirements for a successful claim for interference with privacy as follows: (1) the existence of facts in respect of which there is a reasonable expectation of privacy; and (2) publicity given to those private facts that would be considered highly offensive to an objective reasonable person: para 117 (Gault P and Blanchard J).

> It has been suggested that the concept of a reasonable expectation of privacy is amorphous and ill-defined. I do not consider that anything more precise is either desirable or possible at this stage of the development of the law and at this level of generality…What expectations of privacy are reasonable will be a reflection of contemporary societal values and the content of the law will in this respect be capable of accommodating changes in those values.[37]

1.19 Although these cases involved the development of legal principles through case law rather than by legislation, they still highlight the difficulties of arriving at an overarching definition of privacy. We believe concepts of privacy, autonomy and dignity should underlie any reforms of workplace privacy protection.[38] However, rather than use a broad definition of privacy as the basis for privacy protection, we favour an approach based on addressing particular workplace practices. We think this is a more practical and understandable basis for reform and takes account of the context in which practices occur.

## INFORMATION PRIVACY

1.20 We found that workers are not only concerned about the processes of workplace surveillance, monitoring and testing, but also about what happens to the information collected from these practices. For example, how might a surveillance tape which shows footage of an individual worker be used? Or how may an employer use a worker's photograph? Who might have access to workers' psychological test results? Although such questions raise information privacy issues, we do not focus on information privacy in this Options Paper. Introducing controls on how and why surveillance, monitoring and testing is conducted is likely to overcome some of the potential information privacy issues by limiting the collection of information arising from these processes in the first place.

1.21 Additionally, the privacy of information about workers does receive some, albeit piecemeal, protection in Victoria. There are specific provisions in the *Surveillance Devices Act 1999* (SDA) which make it an offence to communicate or publish material obtained from the use of optical or audio surveillance or tracking

37 *Hosking & Hosking v Simon Runting & Anor* [2004] NZCA 34 (25 March 2004) paras 249–50 (Tipping J).

38 Tipping J indicated that 'It is the essence of the dignity and personal autonomy and well-being of all human beings that some aspects of their lives should be able to remain private if they so wish': *Hosking & Hosking v Simon Runting & Anor* [2004] NZCA 34 (25 March 2004) para 239 (Tipping J).

devices, without the consent of each party involved.[39] However, as we discuss in Chapter 2, the SDA has limited application in the workplace context.[40] The *Information Privacy Act 2000* (IPA) protects personal information (excluding health information) of workers in the Victorian public sector. Health information of Victorian workers (both public and private sector) is protected by the *Health Records Act 2001* (HRA).

1.22 At the federal level, the *Privacy Act 1988* (Cth) (the Privacy Act) protects the privacy of personal information of Commonwealth public sector employees.[41] It also protects personal information about private sector non-employees (such as independent contractors, volunteers and job applicants). However, the Privacy Act does not generally cover small businesses and their workers.[42] Nor does the Privacy Act protect the privacy of personal information which:

- relates directly to the employment relationship between an employer and a current or former private sector employee; and
- is held by the employer in an employee record (this is known as the 'employee records exemption').[43]

The operation of the employee records exemption leaves a significant gap in the privacy protection of workers' personal information, since non-health information about Victorian private sector employees is generally not protected.[44]

---

39 *Surveillance Devices Act 1999* ss 11(1), 11(2)(a).

40 See Chapter 2, paras 2.16–2.17.

41 See the Information Privacy Principles in the *Privacy Act 1988* (Cth) pt III, div 2.

42 The Privacy Act contains a 'small business operator exclusion': ss 6D–6DA, read with s 6C(1). 'Small business operators' are defined as operators of businesses having an annual turnover of less than $3 million: *Privacy Act 1988* (Cth) s 6D(1)(3). The small business operator exclusion from the Privacy Act does not apply to businesses that provide a health service and hold any health information except in any employee record, businesses that disclose personal information about anyone else for a 'benefit, service or advantage' or businesses that provide a 'benefit, service or advantage' to collect personal information about another individual from anyone else: *Privacy Act 1988* (Cth) s 6D(4). Thus these bodies must comply with the provisions of the Privacy Act. A body corporate is not a small business operator if it is related to a body corporate that does not carry on a small business: *Privacy Act 1988* (Cth) s6D(9).

43 *Privacy Act 1988* (Cth) s 7B(3). 'Employee records' are defined in s 6 of the Privacy Act as being 'in relation to an employee…a record of personal information relating to the employment of the employee' and includes information relating to employment terms and conditions, employees' performance or conduct and leave entitlements, union membership and other types of personal information.

1.23 The Privacy Act's employee records exemption has been a source of controversy. The Commonwealth Government indicated soon after the enactment of the Privacy Act that the exemption would be reviewed as part of a general review of the Privacy Act following its second year of operation.[45] The Commonwealth Attorney-General's Department and the Department of Employment and Workplace Relations released *Employee Records Privacy: A discussion paper on information privacy and employee records* for public comment in February 2004. The Discussion Paper posed a range of options in relation to the employee records exemption, including:

- retaining the exemption;
- non-legislative measures such as education, guidelines or policies;
- amendments to the Privacy Act to delete or modify the employee records exemption;
- enacting specific employee records privacy principles; and
- enhancing protection of employee records in workplace relations legislation.[46]

1.24 Responses to that paper were due in April 2004. The Commission will await the outcome of that review before it considers making recommendations on information privacy for workers.

## CONSTITUTIONAL ISSUES

1.25 The Commission's Workplace Privacy terms of reference covers issues that interact with existing federal legislation, which includes the *Privacy Act 1988* (Cth), the *Workplace Relations Act 1996* (Cth) (WRA) and the *Telecommunications Interception Act 1979* (Cth) (TIA).

1.26 This could give rise to certain constitutional issues if a new Victorian Act were found to be inconsistent with a federal Act. In such a case, the Victorian Act would be overridden to the extent that the provisions are found to be

---

44 As discussed in paras 2.16–2.17, the *Surveillance Devices Act 1999* (Vic) may offer some limited privacy protection for information obtained from surveillance.

45 Submission 20.

46 Attorney-General's Department and the Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (2004) 30–34.

inconsistent.[47] Accordingly, it is important to establish how far these federal Acts affect:

- the *practices* of surveillance, monitoring and testing; and
- any *information* created from processes of surveillance, monitoring and testing.

### THE PRACTICES OF SURVEILLANCE, MONITORING AND TESTING

1.27 The Privacy Act deals solely with information privacy. It does not deal with the actual practices involved in undertaking surveillance, monitoring and testing in the workplace.[48] Accordingly, the state is not prevented from legislating on these practices insofar as the Privacy Act is concerned.[49]

1.28 The WRA does not directly deal with such practices either,[50] but it may provide some indirect regulation. Federal industrial agreements, such as certified agreements and Australian Workplace Agreements (AWA), can include clauses on the processes of surveillance, monitoring and testing (for example where surveillance cameras can be used, or when an alcohol and drug testing program can be established).[51] Such clauses are contained in very few federal agreements, but where this is the case they have the force of federal law under the WRA (though they are limited in application to those employees covered by these industrial instruments).[52] These provisions, where they exist, would override any

---

47 *Commonwealth of Australia Constitution Act 1900* (Cth) s 109 which states when a law of a state is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid.

48 Advice provided to the Victorian Law Reform Commission by Simpson, A & Stellios, J, Australian National University, 29 September 2003, 3.3.4—see Appendix 4.

49 Ibid.

50 Simpson & Stellios, n 48, 3.3.4–3.3.6.

51 Simpson & Stellios, n 48, 3.3.5–3.3.6. Examples of certified agreements that look at the use of security video cameras include the National Union of Workers; Transport Workers Union of Australia; and Communications, Electrical Electronic, Energy, Information, Postal, Plumbing and Allied Services Union Australia—Electrical Division and Kodak (Australasia) Pty Ltd (C No 38518 of 1999) Kodak (Australasia) Pty Ltd National Distribution Agreement; and electronic monitoring in the Australian Municipal, Administrative, Clerical and Services Union and Victorian Canine Association Inc (C No 37134 of 1999 Victorian Canine/ASU Inc Enterprise Agreement 1999); provisions on psychological testing are included in the AMP Asset Management Australia Ltd and Financial Sector Union of Australia (C No 26098 of 1998); and generally for Internet and email use policies see Australian Institute of Management—Victoria and Tasmania College of Education and Training Enterprise Agreement 2002 (AG 816954).

52 See *Workplace Relations Act 1996* (Cth) ss 170LZ(1), 170M(1), 170M(2).

state legislation that attempted to cover the same ground.[53] Apart from situations where this has occurred, the state would not be prevented by the WRA from otherwise regulating such processes.[54]

1.29 Finally, the TIA exclusively covers an interception of a communication 'passing over the telecommunications system'.[55] Accordingly, if an employer wants to use a surveillance or monitoring process that involves an interception 'passing over the telecommunications system', it will be covered by the TIA.[56] So the state could legislate to regulate processes that fall outside this definition—namely, if the process occurs prior to or after the communication has 'passed over the system'.[57]

### *Information From Surveillance, Monitoring and Testing Processes*

1.30 As stated above, the provisions of the Privacy Act regulate information privacy generally, including regulation of information relating to job applicants, volunteers and independent contractors. However, the inclusion of the employee records exemption in the Privacy Act (see paragraph 1.22) raises the question of whether any other form of regulation (be it federal or state) could apply to the keeping of employee records. Having considered both the provisions of the Privacy Act and relevant material available at the time the Privacy Act was passed, we have concluded that the employee records exemption was not intended to exclude all other forms of regulation of employee records.[58] Accordingly, we believe the state is free to legislate on this matter. The provisions of the Privacy Act continue to apply to the records of non-employees such as job applicants and independent contractors.

1.31 The WRA also contains regulations dealing with specific types of information held in employee records.[59] This information is used primarily to ensure employers meet their obligations under applicable awards and agreements in facilitating the documenting of breaches of employer obligations (for example, in the correct payment of wages). While the Privacy Act's employee records exemption has no impact on the operation of these regulations, the WRA

53 See *Workplace Relations Act 1996* (Cth) s 170LZ(1).

54 Simpson & Stellios, n 48, 3.3.6.

55 For further explanation of 'passing over the telecommunications system' see n 130.

56 Simpson & Stellios, n 48, 1.3.1.

57 Simpson & Stellios, n 48, 1.4.1.

58 Simpson & Stellios, n 48, 1.1.1, 3.1.1–3.1.12.

59 *Workplace Relations Regulations 1996* (Cth) see Part 9A 'Records by Employers'.

regulations could impinge on the state's ability to legislate for employees, as such regulations would override any state legislation found to be inconsistent with the operation of their provisions. The WRA regulations, however, are limited in application to those workers covered by its provisions.[60]

1.32 The TIA also contains provisions relating to the use of information insofar as it relates to information created from an interception of a communication 'passing over the telecommunications system'.[61] Any information created that falls outside this definition could, in our view, be regulated by the state and would apply consistently to all workers (both employees and non-employees).[62] This information would also be subject to the information requirements contained in the Privacy Act and the WRA.

1.33 Any decision by the Victorian Government to legislate in the area of workplace privacy must take into account the possible implications of the 1996 referral of certain industrial powers by Victoria to the Commonwealth. This is particularly so where the 'practices' and 'information' described above relate to the worker's terms and conditions, and are characterised as industrial issues or arise in the industrial context. This issue is discussed in the next section.

### *REFERRAL OF INDUSTRIAL POWERS TO THE COMMONWEALTH*

1.34 The Commonwealth parliament has a specific list of powers contained in the Commonwealth Constitution with which it can legislate.[63] Similarly, states can legislate on any matters that do not lie within the exclusive legislative power of the Commonwealth parliament.[64] These areas can overlap. The state parliament can also refer one or a number of its powers to the Commonwealth parliament which, in constitutional law terms, is a process called a 'referral of power'.[65]

---

60 *Workplace Relations Regulations 1996* (Cth) pts 9A, 9B are limited in application to employees.

61 *Telecommunications (Interception) Act 1979* (Cth) s 63. See also Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (Cth) which, if passed, may have implications for employers in the use of workers' stored information. The Bill is discussed in para 2.24.

62 Simpson & Stellios, n 48, 1.4.1.

63 Most heads of power are listed in *Commonwealth of Australia Constitution Act 1900* (Cth) ss 51, 52.

64 *Commonwealth of Australia Constitution Act 1900* (Cth) s 107. See also George Williams, *Labour Law and the Constitution* (1998) 3 which details the conferral of power by the state constitutions which confirms the plenary legislative power of the states.

65 For a detailed explanation of the referral process see Graeme Johnson, 'The Reference Power in the Australian Constitution' (1973) 9 (1) *Melbourne University Law Review* 42.

1.35 A referral of power occurred in Victoria in 1996 when the state government referred specific industrial powers to the Commonwealth.[66] None of the powers referred to the Commonwealth specifically include or describe the information or practices raised by the Workplace Privacy reference.[67] Where the state has retained the power, it is able to legislate on these issues.[68] Even where the state has referred a particular power or powers, it is an accepted view that referred powers become concurrent powers that can be used by both the state and the Commonwealth.[69] Accordingly, if the Commonwealth was to legislate in this area, the Commonwealth legislation would override any inconsistent state legislation.[70]

## STRUCTURE OF THE PAPER

1.36 The structure of the remainder of this Paper is as follows:

- Chapter 2 outlines some of the key surveillance, monitoring and testing technologies and practices used in the workplace, and how those practices are currently regulated.
- Chapter 3 examines the gaps in the privacy protection of workers that arise from the use by employers of these practices.
- Chapter 4 proposes options for reform to address the gaps in workers' privacy protection. The Commission has included questions to assist individuals and organisations to make submissions on the options.

66 Williams, n 64, 5.

67 See the terms of reference on page viii, the Agreement Between State of Victoria and Commonwealth of Australia, 30 May 1997 and the *Commonwealth Powers (Industrial Relations) Act 1996*, ss 4, 5.

68 Commonwealth Constitution & Williams, n 64.

69 *Graham v Paterson* (1950) 81 CLR 1, 19.

70 Commonwealth Constitution section 109.

# Chapter 2
# Technologies and Practices

## INTRODUCTION

2.1 Surveillance, monitoring and testing technologies and practices have become significant features in the workplace. The adoption of such practices by employers seems, in part, to be driven by the rapidly changing technological advances in these areas, where workers' terms and conditions are simply modified along the way. This trend has generated considerable anxiety within the community through uncertainty about work terms and conditions as well as the actual nature of these technologies and practices and how they are regulated, if at all. This chapter provides an overview of the key technologies and practices identified by our reference, which are currently in use or which could potentially be used. It also outlines how these practices are currently regulated.

## SURVEILLANCE AND MONITORING

2.2 The terms 'surveillance' and 'monitoring' can mean different things to different people. For example, the Privacy Committee of New South Wales suggested monitoring relates to direct measurements of employee performance, whereas surveillance relates to the observation of activities, sometimes secretly.[71] In this Options Paper, we use the terms 'surveillance' and 'monitoring' interchangeably. In both cases there is the connotation of intentionally watching, listening to, recording or otherwise collecting information about people or objects.[72] This might involve using a video camera to observe a worker, using a

71 Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace* No 67 (1995) 13. See also International Labour Office, *Workers' Privacy—Part II: Monitoring and Surveillance in the Workplace* 12(1) (1993) 12.

72 This could be carried out by the employer or by an agent of the employer.

tape recorder to record a worker's telephone calls, or monitoring the way a worker uses email. Surveillance and monitoring technologies are developing at a rapid rate and are used widely in the workplace. The following are descriptions of some of the more frequently used workplace surveillance and monitoring technologies.

## SURVEILLANCE

### *VIDEO SURVEILLANCE*

2.3 Video surveillance is used in many situations. We see cameras in shops, on public transport and in the entrances to buildings. The Privacy Committee of New South Wales highlighted the extent to which video surveillance is used in Australia in a report in 1995.[73] This report indicated that compared to other industrialised nations, Australia appeared to spend substantially more money per capita on video surveillance equipment.[74]

2.4 The most common type of video surveillance used in the workplace is closed-circuit television (CCTV).[75] It is widely used in retail and other industries to protect property against theft and damage, to protect against unwanted intrusion and for occupational health and safety reasons.[76]

---

73 Privacy Committee of New South Wales, n 71.

74 Ibid 1, 19–20. Estimates of CCTV sales in various countries were provided to the Privacy Committee of New South Wales. For example, CCTV sales in Australia in 1994 were estimated to be A$42m, or approximately A$2.45 per capita. Although per capita sales in Australia were lower than those in the United States (estimated sales of A$4.75 per capita) or the United Kingdom (estimated sales of A$6.15 per capita), the size of the Australian CCTV industry was large compared to other industrialised nations (which had sales of less than A$1 per capita). The Committee provided these statistics as an indication only. They were not intended to be a precise comparison. The Committee also noted it was difficult to obtain statistics on the size of the CCTV market as the information is regarded as commercially sensitive and the measures which are used vary from country to country.

75 'Closed circuit' is a system of transmitting television signals in which the receiving and originating equipment is directly linked by cable, microwave or telephone lines, without broadcasting through the air: <www.eupen.com/glossary/glossarycable.html> at 30 July 2004. CCTV systems vary in complexity. The simplest systems involve a camera connected directly to a monitor. The camera creates the picture that is transmitted to the monitor. A CCTV monitor is similar to a television receiver. The monitor could be located at the employers' premises or some distance away. For more information on CCTV systems, see for example, <www.cctv-information.co.uk> at 30 July 2004. See also para 2.9 for an explanation of how information from video surveillance is captured and used by organisations.

76 Consultation 3.

2.5 Video technology is already sophisticated, and its capabilities are constantly expanding.[77] Video cameras can now 'see' in the dark. They can be set up on motorised platforms that allow them to pan, tilt and zoom.[78] With the addition of a special integrated chip, they can automatically track and record the movement of an individual around a room.[79] They can record at pre-determined intervals or times. Video cameras can also be linked to other business systems such as alarm systems, time management systems and access control systems to form an integrated security network.[80]

2.6 Apart from the increasing sophistication of their capacities, video cameras are becoming smaller, less expensive and more readily available. An array of items containing hidden cameras are available on the market.[81] Some video cameras are small enough to fit into mobile phones and pens and are capable of storing and transmitting images.[82] We were told that video surveillance equipment can be purchased from some retailers for as little as $250.[83]

2.7 Although a vast array of hidden cameras is available, retailers and technical specialists indicated to us that covert video surveillance (ie surveillance which is undertaken without the subject's knowledge) is usually used for a particular reason. For example, if there is a suspicion that someone is stealing, then covert surveillance may be used to identify the culprit and gather evidence.

2.8 In practice, overt video surveillance is more common. Overt surveillance is visible—one of its main functions is to act as a deterrent. Cameras are often placed over cash registers and in other cash handling areas, and at building entries and exits. Retailers may place cameras or monitors in obvious positions so customers

77 For example, technology is moving from analogue to digital. Having video information in digital format opens up an array of processing capabilities available on a basic personal computer such as real-time analysis and automation. There is no need for video tapes and it is much easier to search and edit the information.

78 'Pan (panning) refers to the capacity of a video camera to move across the sweep of an area to view a wide area. Tilt (tilting) refers to the capacity of a video camera to adjust its angle through an upward, downward or sideways tilt of the main camera unit. Zoom (zooming) refers to the capacity of a video camera to focus on a distant object or activity and provide a magnified view.': Privacy Committee of New South Wales, n 71, 17.

79 Frederick Lane, *The Naked Employee: How Technology is Compromising Workplace Privacy* (2003) 119.

80 See Australian Security Industry Association at <www.asial.com.au> at 30 July 2004.

81 For example, a search of the Internet using the term 'hidden camera' reveals that surveillance cameras can be disguised in items such as radios, smoke detectors, clocks and even handbags.

82 Consultation 3.

83 Ibid.

and staff can actually see themselves under surveillance in a store. There is even a market for 'dummy' cameras.[84]

2.9 The way information obtained from video surveillance is captured and used varies from organisation to organisation. Larger organisations may have banks of video monitors constantly watched by security personnel. Other organisations may not have personnel watching the monitors, but may have video footage captured on tape. In these circumstances, the tapes may be stored for a certain period[85] and only reviewed if there is an incident. It is common for video images to be taped on a continuous loop or directly stored on computer hard disks as a digital data file.[86] Although storage of video footage is currently expensive, market demand is leading to cheaper, more efficient ways of storing it.[87]

2.10 It is likely that video surveillance technology will be combined with other technologies. It can already be cross-matched with face recognition technology. Research is being undertaken into characterising individuals by their mannerisms to overcome difficulties with existing face recognition technology.[88]

### *AUDIO SURVEILLANCE*

2.11 The most common type of audio surveillance in the workplace is telephone monitoring.[89] It is widely used in businesses which rely on the telephone, such as call centres, insurance companies, telecommunications companies, banks and stockbrokers.[90] Participant monitoring is the term which is generally used for this kind of monitoring. It means listening to, or recording a communication over the telecommunications system by a party to the conversation, or a person or organisation related to that party.[91] In the workplace, this generally means the monitoring of a worker's telephone conversation (usually

84 Ibid.

85 There is no set time for keeping tapes; the length of time for which video tapes are kept varies from organisation to organisation: ibid.

86 Ibid.

87 For example, computer storage is cheaper than storage on video tapes: ibid.

88 Ibid.

89 Ibid.

90 There are legal requirements for a bidder or target company to record telephone calls with shareholders about a takeover bid which are made during the bid period of a company takeover: see *Corporations Act 2001* (Cth) ss 648J–648U.

91 See Australian Communications Industry Forum, *Industry Guideline: Participant Monitoring of Voice Communications* ACIF G516:2004 (2004) 5.

between a worker and a customer) by the worker's employer. Participant monitoring can be undertaken in a number of ways. One way of listening in to a telephone conversation is by 'double jacking' the telephone line.[92] As this kind of monitoring occurs when a communication is passing over the telecommunications system, it is covered by the provisions of the *Telecommunications (Interception) Act 1979* (Cth).[93] However, it is not so clear that other types of telephone call recordings are covered by the Telecommunications (Interception) Act. For example, it is not clear whether the recording of a person's voice on the telephone by equipment, such as a tape recorder which is external to the telephone system, constitutes an interception.[94]

2.12 Any form of audio surveillance which does not involve a communication passing over the telecommunications system can be regulated by the Victorian Government. The tape recording of a conversation (which does not involve the telephone system) would fall into this category, as might the recording of sound in conjunction with video footage.

### *TRACKING TECHNOLOGIES*

2.13 Tracking devices using Global Positioning System (GPS) technology are becoming more widespread. The term 'Global Positioning System' refers to a group of satellites that constantly orbit the earth emitting radio signals.[95] Small units called GPS receivers, which can be installed in anything from vehicles to mobile phones, use the radio signals to pinpoint the location of the object in which they are installed.[96]

2.14 Employers in the transport industry use GPS technology to collect information about company vehicles including location, distance travelled, speed, travel time, idle time, fuel consumption and time at locations.[97] Information

92 'Double jacking' involves adding an additional 'eavesdropping' link to an existing voice circuit. A jack refers to a plug on the end of connecting wires used in old style exchanges to connect circuits for a call. A double-jack is simply an extra connection to the circuit or call, allowing the person connected to the second jack to listen in on the conversation. In a modern exchange, digital switching enables this to be done without ever having to physically connect a wire.

93 See the discussion of constitutional issues in Chapter 1, paras 1.25–1.35.

94 For a discussion of this issue, see R Magnusson, 'Privacy, Surveillance and Interception in Australia's Changing Telecommunications Environment' (1999) 27 (1) *Federal Law Review* 51.

95 Lane, n 79, 199.

96 Ibid.

97 Submission 18.

obtained from GPS can be downloaded and superimposed on a map to plot a vehicle's route[98] or used to generate reports regarding the movement of vehicles over a particular period.[99] Devices which can be located in a vehicle's suspension and which measure vehicle speed and weight can be linked to the information obtained from GPS. This can be used to determine whether cargo has been loaded or unloaded at an unexpected time or location.[100]

2.15 In a submission to the Commission, a supplier of vehicle information systems which use GPS technology said the benefits to transport companies of using such systems include improved safety, productivity and competitiveness through maximising vehicle and driver utilisation.[101] However, tracking this information about vehicles can also indirectly reveal information about a worker's movements and performance outside work hours.

### *REGULATION OF SURVEILLANCE*

2.16 The Surveillance Devices Act (SDA) provides some protection against surveillance of workers.[102] It makes it an offence for a person to install, maintain or use an optical surveillance device[103] or listening device[104] to record private activities and conversations to which they are not a party, without the consent of

98 Consultation 3.

99 Submission 18.

100 Consultation 3.

101 Submission 18.

102 See also the discussion of the regulation of telephone monitoring by the *Telecommunications (Interception) Act 1979* (Cth) in para 2.11.

103 An 'optical surveillance device' means any device capable of being used to record visually or observe a private activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment: *Surveillance Devices Act 1999* s 3(1). The word 'private' is removed from this definition by s 5(1) of the *Surveillance Devices (Amendment) Act 2004*, but the term 'private' remains in the substantive provisions of the Surveillance Devices Act. As such, this does not alter the regulation of the installation, use and maintenance of optical surveillance devices. At the time of writing the Surveillance Devices (Amendment) Act was not yet proclaimed.

104 A 'listening device' means any device capable of being used to overhear, record, monitor or listen to a private conversation or words spoken to or by any person in private conversation, but does not include a hearing aid or similar device used by a person to overcome the impairment and permit that person to hear only sounds audible to the human ear: *Surveillance Devices Act 1999* s 3(1). The word 'private' is removed from this definition by s 5(1) of the *Surveillance Devices (Amendment) Act 2004* but the term 'private' remains in the substantive provisions of the Surveillance Devices Act. As such this does not alter the regulation of the installation, use and maintenance of listening devices. At the time of writing the Surveillance Devices (Amendment) Act was not yet proclaimed.

the participants.[105] It also makes it an offence to communicate or publish material obtained from using these devices without the consent of each party involved.[106] The prohibition against communication and publication applies even if the person publishing the information is a party to the private activity or conversation.[107] Restrictions are also imposed on the use, installation and maintenance of tracking devices[108] without the consent of the person whose location is being tracked and the communication of information obtained from their use.[109] Certain law enforcement activities are exempted from these prohibitions.[110]

2.17 There are two significant limitations to the application of the SDA. First, it does not apply to the use of devices where the person subject to surveillance has agreed to it.[111] The difficulties with the concept of consent in the workplace context are discussed in Chapter 3, paragraphs 3.60–3.68. Secondly, the regulation of listening and optical surveillance devices only applies where the conversations and activities being monitored ought reasonably to be expected to be private.[112] The definitions of 'private activity' and 'private conversation' are restrictive.[113] As a result, in most situations, workers will often be unable to rely on

105 *Surveillance Devices Act 1999* ss 6(1), 7(1).

106 *Surveillance Devices Act 1999* s 11(1)(2)(a).

107 *Surveillance Devices Act 1999* s 11(2)(a).

108 A 'tracking device' means any electronic device, the primary purpose of which is to determine the geographical location of a person or an object: *Surveillance Devices Act 1999* s 3(1).

109 *Surveillance Devices Act 1999* ss 8(1),11(1)(2)(a). Section 5(1) of the *Surveillance Devices (Amendment) Act 2004* extends the ambit of the principal act to also cover a combination of optical surveillance devices, listening devices and tracking devices and any devices prescribed as surveillance devices. At the time of writing the Surveillance Devices (Amendment) Act was not yet proclaimed.

110 A warrant or emergency authorisation is required for the installation, use or maintenance of these surveillance devices or their installation, use or maintenance must be authorised by a law of the Commonwealth: *Surveillance Devices Act 1999* ss 6(2), 7(2)(a)(b), 8(2). These provisions have been extended by sections 5 and 7(b) of the *Surveillance Devices (Amendment) Act 2004* to also cover corresponding warrants or corresponding emergency authorisations issued under corresponding surveillance devices laws of other jurisdictions. (At the time of writing the Surveillance Devices (Amendment) Act was not yet proclaimed.) Additionally, under the *Surveillance Devices Act 1999*, a law enforcement officer can install an optical surveillance device if it is authorised by an occupier of premises and this is necessary for the protection of the person's lawful interests: s 7(2)(c).

111 *Surveillance Devices Act 1999* ss 6(1), 7(1), 8(1). The consent may be either express or implied.

112 *Surveillance Devices Act 1999* ss 6(1), 7(1) read with s 3(1).

113 The SDA has limited application to employers' use of surveillance devices in the workplace because most activities and conversations will not come within the definition of private conversations or activities. For example, a private activity is defined in section 3(1) as an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it only to be heard

the SDA to protect them against surveillance in the workplace. However, the information an employer may collect through the use of surveillance devices may still be subject to the provisions of information privacy laws. As we explain in Chapter 1, the scope of these laws is limited.[114]

## EMAIL AND INTERNET MONITORING

2.18 Email and Internet monitoring is one of the most widespread forms of workplace monitoring. Surveys have revealed that around 76% of employers monitor their workers' email content periodically for maintenance and troubleshooting or where email abuse is suspected. Around 5% monitor regularly. Of those who monitor, 65% undertake monitoring without notification.[115] Email and Internet monitoring is also used to protect the integrity of computer systems from breach of protocols and the introduction of viruses and worms.[116]

2.19 Many employers use 'filtering' or 'blocking' technologies to prevent workers accessing particular types of material on the Internet.[117] For example, an employer may block access to pornographic websites, or may prevent workers accessing websites containing particular words or phrases.[118] Employers may also block spam,[119] as well as email messages of certain sizes or types.[120]

2.20 Also available are monitoring technologies which enable an employer to record or inspect workers' email and Internet activity, either as it happens or afterward. Interestingly, monitoring technologies cannot generally separate personal emails from work-related emails.[121] Some technologies have the capacity

---

by themselves, but does not include (a) an activity carried on outside a building; or (b) an activity carried on in circumstances in which parties to it ought reasonably to expect that it may be observed by someone else.

114 See the discussion of information privacy laws in Chapter 1, paras 1.20–1.24.

115 Freehill, Hollingdale & Page, *Internet Privacy Survey Report* (2000) 9. See also PricewaterhouseCoopers, *Privacy Survey 2000* .

116 Moira Paterson, 'Monitoring of Employee Emails and other Electronic Communications' (2002) 21 (1) *University of Tasmania Law Review* 1 7.

117 NetAlert and the Australian Broadcasting Authority, *Effectiveness of Internet Filtering Software Products* (2001) 5.

118 See ibid 5–10 for more information about 'blocking' and 'filtering' technologies.

119 'Spam' is the term used to define unsolicited 'junk' email sent to large numbers of people for promotional purposes. It can also refer to inappropriate promotional postings to discussion groups or bulletin boards. See <www.getnetwise.org/glossary> at 5 April 2004.

120 Consultation 1.

121 Ibid.

to record all a worker's email and Internet activity; others raise an alert if, for example, a worker accesses an inappropriate website.[122] Certain technologies allow an employer to inspect the contents of an email message or website; others only inspect the email header (ie subject, sender, recipient, size and so on) or website address.[123] Some monitoring conducted by employers is 'after the fact', that is employers inspect files stored on a worker's computer or kept in the employer's back-up, mail or proxy servers.[124] Other monitoring may be in 'real time'. Real time monitoring is often used by IT help desks. It allows the help desk staff to log on to an individual's computer. This is of great assistance when a computer user has a problem in the workplace, but it can also be done without their knowledge.[125]

2.21 Information obtained from monitoring activities can be presented in various ways. Depending upon the product used, reports can be provided that reveal the activities of specific workers, or grouped in a way that individual workers are not identified.[126]

2.22 Email and Internet monitoring activities are generally carried out in larger organisations by IT professionals, usually a network administrator. Network administrators and other IT professionals require a high degree of access to organisations' computer systems to effectively manage the systems.[127]

### *REGULATION OF EMAIL AND INTERNET MONITORING*

2.23 Employer email monitoring does not appear to be covered by the SDA, though there are provisions in it which cover the installation, use and maintenance of a 'data surveillance device'. Under the SDA, there are no controls on the use, installation or maintenance of a 'data surveillance device' in relation to computer use except where this is done by a law enforcement officer. When this occurs, the officer must have the consent of the person on whose behalf information is 'inputted or outputted' from the computer, unless the officer has a warrant or

122 Andrew Schulman, 'Computer and Internet Surveillance in the Workplace' (2001) 8 (3) *Privacy Law and Policy Reporter* 49 51.

123 Ibid.

124 Ibid 52.

125 Consultation 1.

126 Schulman, n 122, 52.

127 Consultation 1.

emergency authorisation.[128] The Act does not prevent an employer from installing or using a 'data surveillance device' or authorising a law enforcement officer to do so. In the latter case, the employer could authorise the law enforcement officer to install the device as it would be the employer on whose behalf the information is being 'inputted or outputted' from the computer.

2.24 There has also been considerable uncertainty as to whether the *Telecommunications Interception Act 1979* (Cth) (TIA) regulates monitoring of emails and other types of messages such as voicemails and short message service (SMS). Employer monitoring of communications is not prohibited in the usual situation where the employee is aware of the monitoring.[129] The reading of an email or the monitoring of Internet usage may not be covered by the TIA as it may not be considered to be the interception of a communication 'passing over a telecommunications system'.[130] In an attempt to clarify the application of the Telecommunications (Interception) Act, the Commonwealth Government has introduced an amending Bill[131] which excludes 'stored communications' from the current prohibition against interception of communications.[132] 'Stored

128 *Surveillance Devices Act 1999* ss 9(1)(2). Section 7(b) of the *Surveillance Devices (Amendment) Act 2004* extends this provision to include corresponding warrants and corresponding emergency authorisations. See n 110 for more information about corresponding warrants and corresponding emergency authorisations.

129 *Telecommunications (Interception) Act 1979* (Cth) s 6(1). The interception of communications is also not prohibited where it is done on the premises of the employer by use of equipment that is part of the service provided by the telecommunications carrier: s 6(2). There is some authority to suggest that even when employees are not aware their telephone conversation is being recorded by their employer, the recording may not be an interception under the *Telecommunications (Interception) Act 1979* (Cth) if it occurs when the employee is acting in the course of their employment: see *R v Evans* (1999) 152 FLR 352.

130 Between the sender and intended receiver of an email, the message may 'sit' on a network or Internet Service Provider's server. If 'passing over' is considered to be the passage from the sending to the receiving computer, then access of the email as it is 'sitting' on a server may be an 'interception'. If, however, 'passing over' were limited to the transmission of the message in the cables or optic fibres, then the access of an email when it is on the server would not be considered to be an 'interception'. There is another point of doubt with respect to emails relating to the nature of a 'telecommunications system'. It is unclear from the Act whether a networked computer system in a workplace would be considered to be a single entity or a 'telecommunications network' separate from the carrier's telecommunications network. If it is a separate network made up of a number of computers, then the access of emails in the workplace may be subject to the Act.

131 Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (Cth).

132 Commonwealth, *Parliamentary Debates*, House of Representatives, 27 May 2004, 29130 (Philip Ruddock, Attorney-General). A 'stored communication' is a communication stored on equipment or any other thing, but does not include a Voice over Internet Protocol (VoIP) communication or any

communications' would include stored email, voicemail and SMS messages.[133] The Bill provides that these provisions will cease to have effect 12 months after their commencement. The 12-month period is to allow time for a more comprehensive review of Australia's interception regime.[134]

2.25 The Federal Privacy Commissioner has issued 'Guidelines on Workplace E-mail, Web Browsing and Privacy',[135] but they are not compulsory.

## BIOMETRICS

2.26 'Biometrics' is the science of identifying people on the basis of physical or behavioural characteristics.[136] Examples of biometric identifiers include DNA, fingerprints, irises, facial characteristics, voice and hand geometry.

2.27 Biometrics is a statistical science. It works by comparing the characteristics of a person which are stored in a database to a new sample provided by that person. It can be used to initially *identify* someone by comparing the characteristic provided by that person with all stored characteristics (a one-to-many comparison). Or it can be used to *verify* that a person is who they say they are by comparing the previously stored characteristic to the fresh characteristic (a one-to-one comparison).[137] Biometric identifiers cannot be lost or forgotten like other forms of identification, and are seen by supporters as a good way of controlling access to buildings, airports and computer networks.[138] They are also seen as a way

---

other communication held in storage on a highly transitory basis and as an integral function of the technology used in carrying the communication: Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (Cth) schedule 1, clause 4. According to the Explanatory Memorandum to the Bill, VoIP is a form of packet-switched data communication that involves converting audible sounds into data packets for transmission over a telecommunications system. VoIP has been excluded from the definition of stored communications because VoIP data packets may be stored for only a fraction of a second while the data is in transit: Explanatory Memorandum, Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (Cth), 4.

133 Explanatory Memorandum, Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (Cth), 5–6.

134 Commonwealth, *Parliamentary Debates*, House of Representatives, 27 May 2004, 29130 (Philip Ruddock, Attorney-General).

135 Available from <www.privacy.gov.au> at 30 July 2004.

136 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (2003) 44.

137 Ibid.

138 'Prepare to be Scanned', *The Economist Technology Quarterly* 6 December 2003 15.

of reducing 'buddy-punching' in the workplace—that is, the ability of workers to clock on and off for each other.[139]

2.28 The use of biometrics in the workplace is still rare.[140] But it is likely to become more common as the technology becomes more reliable and decreases in cost, particularly with the prevalence of security concerns in the community.[141] However, at the moment pin numbers and passwords are still regarded by some as better security alternatives.[142]

2.29 One of the issues with biometrics is that, regardless of the method, extracted biometric data is typically different every time it is used, even for the same individual using the same method. The match between the stored data and new data provided by the individual will never be exact. Biometrics systems work on the basis of probabilities. The extent to which a system might register false positives (ie where a person is incorrectly identified as someone else) or false negatives (ie where a person who is meant to be identified by the system is not identified) depends on the tolerance limit set for the desired error rates. For example, if a high tolerance limit is set, fewer legitimate users will be falsely rejected by the system, but the probability that an illegitimate user will be accepted by the system is higher. If the tolerance limit is set low, the rejection rate for legitimate users would be high, but the likelihood that illegitimate users would be rejected is also high. Setting the tolerance limits is a delicate balance that is different for each type of biometric measure and system installed.

2.30 Accessibility to biometric systems is also problematic for segments of the population. This is strikingly demonstrated in the case of finger scanning. Between 4% and 5% of the population will not have an acceptable finger scan due to having fingerprints that are genetically indistinct or that have been worn down

139 Ibid 16.

140 A recent example of a trial of a biometric system in the workplace was Qantas' attempt to introduce a finger-scanning system to log baggage handlers clock-on and clock-off times. The trial was opposed by the Transport Workers' Union (TWU) as an invasion of privacy. Discussions between Qantas and the TWU in the Australian Industrial Relations Commission resulted in Qantas agreeing to introduce electronic swipe card time and attendance system: 'Qantas abandons finger-scans', <www.news.com.au> at 1 June 2004.

141 Consultation 3.

142 This is mainly due to cost issues at present. Biometric systems are expensive compared with other security measures such as passwords and pin numbers. See *The Economist Technology Quarterly*, n 138, 15.

through manual work.[143] Such individuals would not be able to use a system relying on finger scanning alone.

2.31 One of the concerns that individuals express about biometrics is the ability to match caught information with other information to form a profile of an individual. This is not currently possible due to incompatibility between the various means of capturing biometric data and the storage databases.[144] However, this may also change in the future.

### *REGULATION OF BIOMETRICS*

2.32 There is uncertainty about whether biometrics is regulated by the SDA as the Act's definitions of what constitutes 'surveillance devices' are quite specific and may not be capable of covering biometric technologies. For example, it is not clear whether a biometric device such as an iris camera or finger scanning technologies used to clear people for entry into a building come within the SDA definitions of various surveillance devices. If they do not fall within the definitions, then the SDA does not regulate their use.[145]

2.33 The Biometrics Institute has recently issued a draft Privacy Code for the biometrics industry.[146] However, if introduced, the code would only bind members of the Biometrics Institute, and membership is voluntary.

---

143 See *The Economist Technology Quarterly*, n 138, 16.

144 Consultation 3.

145 For example, it is not clear whether an iris camera used for building access falls within the definition of an 'optical surveillance device' or a 'tracking device.' See n 103 for a definition of an optical surveillance device and n 108 for the definition of a 'tracking device'. It is not clear that an iris camera fits within this definition. If the camera is permanently mounted in a workplace, particularly if it has a limited focal length, then it may not be capable of recording or observing any activity, that is, the limitations of the camera lens may prevent it from 'observing' or 'recording' any meaningful images of an activity occurring beyond the focal length of the camera. The camera could perhaps be seen as a 'tracking device' as it is an 'electronic device the primary purpose of which is to determine the geographical location of a person or an object'. That is, to be a tracking device, the primary purpose of the iris camera would have to be to verify that an authorised person, identifiable through its stored data, is standing in a particular location—in front of the camera. If the person consents to the use of the iris camera, then the SDA would not apply.

146 The Biometrics Institute is an independent not-for-profit membership organisation. Its membership consists of government and business users and vendors of biometric services and products. See <www.biometricsinstitute.org> at 30 July 2004. The draft code is available from this website. At the time of writing, the code was awaiting approval by the Federal Privacy Commissioner.

### OTHER MONITORING PRACTICES

2.34 Other monitoring practices which were mentioned to us during consultations included the use of mystery shoppers, swipe cards, scan rate monitoring and keystroke monitoring.

2.35 Mystery shoppers are people who pretend to be customers to assess a worker's performance. The worker does not know the mystery shopper is not a genuine customer. Mystery shoppers are used extensively in the retail and service industries. We were also told they are sometimes used to prevent theft.[147]

2.36 Swipe cards are generally used to access a particular building or area. The information obtained from a swipe card can be used to determine whether a worker is at work or in a certain area of a building. This could be regarded as a form of surveillance, but it is uncertain whether the use of a swipe card is regulated by the SDA (refer to discussion of regulation of biometrics and the SDA in paragraph 2.32—the issues are similar in relation to swipe cards).

2.37 Scan rate monitoring and keystroke monitoring are ways of measuring a worker's productivity. Scan rate monitoring is used in the retail industry as a means of measuring the speed at which items are scanned through a register.[148] Keystroke monitoring involves the use of software or a device to record every keystroke a computer user types on a keyboard.[149] Keystroke monitoring was referred to in the context of measuring the performance of workers in call centres.[150] The issues arising from using surveillance and monitoring practices to measure productivity are discussed in Chapter 3.

## TESTING

### MEDICAL TESTING

2.38 Although there is surprisingly little literature available on general medical or health testing, the medico-ethical framework surrounding this form of testing sets the scene for all other forms of testing raised by this reference.

147 Consultation 6.

148 Consultation 6.

149 Lane, n 79, 128.

150 Consultation 8.

### *PREVALENCE*

2.39 There is scant statistical evidence available indicating the levels of medical testing within the Australian community. In a response to an International Labour Organisation questionnaire on maternity protection, the Commonwealth Government stated 'many workplaces require potential employees to have a medical examination prior to being permanently appointed'.[151] In its 2001 report into hepatitis C-related discrimination, the Anti-Discrimination Board of NSW stated 'pre-employment medical assessments are a relatively common part of recruitment practice'[152] and evidence indicates that 'pre-employment medicals are often required of prospective employees prior to culling candidates for interview'.[153] In the same year, a United States survey found 68% of major firms required medical examinations of both new and current employees.[154]

### *PROCESS OF TESTING*

2.40 The two circumstances in which an employer could require an existing employee to undertake a medical test are if the employee simply agreed to it (in their contract or otherwise) or if the employee's federal industrial instrument expressly allowed for it. An employee is only required to obey a lawful and reasonable order of the employer.[155] If the employee refused to be tested, and the employer still compelled the testing, this may breach the employer's implied duty of trust and confidence,[156] and in doing so breach the employee's contract.[157] In

151 'ILO and Pre-Employment Pregnancy Testing' (1999) 106 *Unity News: Weekly News Summary* .

152 Anti-Discrimination Board of New South Wales, *C Change: Report of the Enquiry into Hepatitis C Related Discrimination* (2001) 60.

153 Ibid 61.

154 American Management Association, *2001 AMA Survey on Workplace Testing: Medical Testing* Summary of Key Findings (2001).

155 Employees owe employers an implied 'duty to obey the employer's lawful and reasonable orders'. In assessing if an order is lawful and reasonable, the court will look to whether the practice falls within the scope of the contract, and whether it was also reasonable 'in all the circumstances', see Creighton and Stewart, n 18, 248.

156 In the English case of *Bliss v South East Thames Regional Health Authority* [1985] IRLR 308 a surgeon was suspended for refusing to undertake a psychiatric examination required by his employer. The evidence did not indicate presence of psychiatric problems, but rather of a personality clash. At 314–15, Dillon LJ in the majority observed 'There is no general power in an employer to require employees to undergo psychiatric examination', and that 'it would be difficult, in this particular area of employment law, to think of anything more calculated or likely to destroy the relationship of confidence and trust which ought to exist between employer and employee'. This lack of 'general power' to require a psychiatric examination can arguably be applied more broadly to other forms of

the pre-employment context there seems to be even less restraint on an employer compelling such tests. There are of course limitations imposed by laws prohibiting unlawful discrimination.[158]

## Content of Test

2.41 Once the employer has decided to require a medical test, there is no 'standard' medical or health test that doctors are required by law to administer.[159] Rather, what is tested is mostly left to the doctor's professional judgment.[160] The underlying reasoning for this position is that to be overly prescriptive about the elements of a medical test not only undermines a doctor's professional ability to judge and conduct the tests required of the position, but would restrict the flexibility required to test for a diversity of job positions. Our consultations revealed that it was quite common for employers not to provide the inherent requirements[161] of the job to doctors, with the consequence that broader, more

---

testing, as well as surveillance and monitoring more generally. This case has been applied in Australia —see *Burazin v Blacktown City Guardian Pty Ltd* (1996) 142 ALR 144. The term of implied trust and confidence has itself been adopted in a number of Australian cases, eg see *Hail Creek Coal Pty Ltd v CFMEU* P935309, 12 July 2004 per AIRC Full Bench; *Patty v Commonwealth Bank of Australia* (2002) 113 IR 36; *Thomson v Orica Australia Pty Ltd* (2002) 116 IR 186; *Jager v Australian National Hotels Pty Ltd* (1998) 7 Tas R 437 at 457 per Slicar J; *AMFEPKIU v NSW Sugar Milling Co-operative Ltd*, Print P9636, 25 March 1998 per Munro J; *Hinds v Laser Resources Management Pty Ltd*, PR914451, 21 February 2002 per Hingley C.

157 For a detailed discussion of the implied duty of trust and confidence and the potential ramifications of breaching the duty see Kelly Godfrey, 'Contracts of Employment: Renaissance of the Implied Term of Trust and Confidence' (2003) 77 *Australian Law Journal* 764.

158 See for example the *Equal Opportunity Act 1995* ss 22, 23 which sets out when employers may deny employment if the person cannot perform the genuine and reasonable requirements of the position, and how the employer may set reasonable terms of employment (at the federal level, section 15 of the *Disability Discrimination Act 1992* (Cth) refers to the ability of the employee to perform the inherent requirements of the position and considers any 'unjustifiable hardship' to the employer). Otherwise, anti-discrimination laws set out lists of attributes which protect people from unlawful discrimination (see for example section 6 of the *Equal Opportunity Act 1995)*. If the workplace medical test was used to discriminate on the basis of one of these attributes, and did not fall under an exception/exemption, this could constitute unlawful discrimination in either the employment (section 14) or pre-employment (section 13) context. Some of the attributes listed in the *Equal Opportunity Act 1995* are listed in federal anti-discrimination laws which also contain similar provisions covering employment and pre-employment contexts.

159 Consultation 9.

160 Consultation 9.

161 For a detailed discussion of what constitutes the 'inherent requirements of the position' see Australian Centre for Industrial Research and Training, *Fitness for Duty—Recent Legal Developments* Working Paper 69 (2001) 15–18. See also *Hail Creek Coal Pty Ltd v CFMEU* P935309, 12 July 2004 per Full Bench discusses 'inherent requirements ' at para 124: 'the phrase "inherent requirements" has been

invasive tests were administered than might have actually been required.[162] Interestingly, an emerging trend identified in consultations was that requests by employers for the inclusion of a 'mental health' assessment as a component of a medical examination were becoming increasingly common.[163]

## Relationship Between Doctor and Worker

2.42 The process of medical testing itself is governed by medical ethics,[164] but the ethics underpinning the doctor–patient relationship are in some doubt where the testing is conducted for the purpose of a job related 'medical assessment'. The Australian Medical Association (AMA) position statement on Independent Medical Assessments on Behalf of Parties Other than the Patient (1998 as amended 2000) states:

> Medical practitioners are requested to assess persons on behalf of third parties such as insurance companies and employers. In these circumstances, a traditional doctor/patient therapeutic relationship does not arise. The role of the medical practitioner in these assessments is to provide an impartial medical opinion. It is not to treat the person. The result of the assessment is a report to the third party, not to the person or the person's treating medical practitioner.[165]

---

judicially considered to mean something that is essential to the position. To determine what are the inherent requirements of a particular position usually requires an examination of the tasks performed, because it is the capacity to perform those tasks which is an inherent requirement of the particular position'.

162 Consultation 9.

163 Consultation 9.

164 See Australian Medical Association, *Code of Ethics* (May 2003).

165 See Australian Medical Association, *Independent Medical Assessments on Behalf of Parties Other Than the Patient: 1998 as Amended 2002* AMA Position Statement (2002). The AMA does advise gaining a person's explicit consent to the assessment, particularly where it is an intimate assessment or the taking of tissue samples is involved. See also Australasian Faculty of Occupational Medicine, *Guidelines for Health Assessments for Work* (1998) 16–18, which in contrast to the AMA states 'All medical conditions should not necessarily be disclosed to the employer, nor, for that matter, every relevant aspect to the employment situation, if a reasonable course of action to fulfil the responsibilities of ensuring workplace safety can be taken…The person must be advised of the necessity for disclosure of any medical condition or disability which the examining doctor or nurse considers will be necessary to discuss with the employer…The person must be allowed to express their own opinion and be permitted to enquire about any alternative course of action with the doctor or nurse. A compromise may be reached about what information can be passed on. Access to medical records in a pre-placement health assessment do not have the same status as medical records kept by a medical practitioner, or other health professional…The ownership that is considered to be that of the doctor or nurse, if functioning in a private practice, but that of the organisation if the doctor or nurse is employed or contracted by an organisation. In the latter situation, the doctor or nurse is considered

2.43 This distinction between 'medical assessor' and 'doctor' is particularly pertinent considering the trend toward using company or company-selected doctors.[166] In fact, Australia Post recently attracted publicity when it required certain workers, who had provided medical certificates from family doctors, to re-submit to a medical assessment by a company-selected doctor.[167]

2.44 The law on the duties owed by the doctor in this context is not entirely clear. It has been established that a doctor has a duty of confidentiality and a duty not to injure.[168] It is less clear, and more dependent on the particular fact scenario, whether or not a doctor has a duty to inform the examinee of results or an undiagnosed condition.[169] This has implications for the disclosure of medical results where, subject to the examinee's prior consent to the test,[170] results may be disclosed solely to the employer or potential employer. We were advised that the arrangement between the doctor and the employer (which may require the doctor not to disclose any information to the examinee) is similarly unregulated, and is often governed by informal contractual arrangements.[171] In these circumstances, problems may arise with a worker's actual ability to genuinely consent to such arrangements—this is discussed in detail in Chapter 3, paras 3.60–3.68.

2.45 In addition, our consultations suggest that with a medical examination, particularly where the doctor is not the worker's treating doctor, the analysis mostly stops at the point where a 'vulnerability' to a condition can be ascertained.[172] An assessment of 'vulnerability' could conceivably be contested by a worker who is denied an opportunity or position on this basis, in the situation

---

the "custodian" of the medical records, and must ensure the privacy of the information through ethical practice'. It should also be noted that some companies have the practice of engaging company nurses (as distinct from doctors) who are governed by similar ethical obligations—see Australian Nursing Council, Australian Nursing Federation and Royal College of Nursing, Australia, *Code of Ethics for Nurses in Australia* (Revised 2002) and the Australian Nursing Council, *Code of Professional Conduct for Nurses in Australia* (2003).

166 Consultation 9.

167 *'Postal Workers Reject New Sick Leave Policy'* (2003) ABC Online: 9 December 2003 .

168 Victor Harcourt, 'The Doctor, the Third Party and the Examinee: Is There a Duty to Inform' (2000) 8 *Torts Law Journal* 221 240.

169 Ibid 221, 241–3. We were informed that if a serious condition requiring treatment or endangering the patient or a third party is discovered during a workplace medical assessment, the doctor is under a clear duty (a duty of care) to communicate the information to the patient or the patient's doctor: Dr Ian Freckelton, barrister, Consultation (28/06/04).

170 AMA, n 160.

171 Consultation 9.

172 Consultation 9. See also ALRC Report, n 19.

where an existing treatment or management regime is not taken into account, or where the 'vulnerability' is of a low risk.

## Consent/Confidentiality

2.46 Concepts of consent, confidentiality and legal authority[173] underpin medical testing. Within the usual doctor–patient context, confidentiality is characterised as a 'relationship between practitioner and patient…which imposes special obligations on the doctor to act only in the patient's best interests'.[174] As discussed, the uncertainty about the relationship in a testing situation leaves the nature and extent of this duty in question. The AMA advises medical assessors that 'the person's explicit consent to the assessment must be obtained before proceeding'.[175] Yet the form of consent is not specified[176] and it is unclear whether the individual will be aware of the level and detail of disclosure that may be provided to the employer. As such, the protections to the individual that may be assumed to exist in the doctor–patient context seem far from guaranteed.[177]

### *REGULATION*

2.47 The Equal Opportunity Commission of Victoria (EOCV) has released pre-employment medical testing guidelines which refer to the main features of non-discriminatory medical testing.[178] However, the EOCV guidelines are

173 Suzie Laufer, 'Medico-Legal Conference on Individual Testing and Review, Bond University, June 1991' (1991) 65 *Australian Law Journal* 584.

174 Moira Paterson and Ea Mulligan, 'Disclosing Health Information Breaches of Confidence, Privacy and the Notion of the "Treating Team"' (2003) 10 *Journal of Law and Medicine* 460 4, 61.

175 Australian Medical Association, *Independent Medical Assessments on Behalf of Parties Other Than the Patient: 1998 as Amended 2002* AMA Position Statement (2002) 1–2.

176 It was suggested in a consultation that clear enunciation of the ambit of the waiver in the form of written information to the patient would be constructive: Dr Ian Freckelton, barrister, Consultation (28/06/04).

177 Ibid, the Commission has been informed that the Medical Practitioners Board of Victoria has recently convened a Forensic Issues Working Party, the aim of which will be to produce comprehensive guidelines for Victorian doctors when conducting forensic assessments, as well as engaging in other activities that possess a forensic purpose or component (ie an assessment for a court or litigation-related purpose). This could impact on how work-related assessments are conducted.

178 See Equal Opportunity Commission Victoria, *Employer Guidelines: Pre-Employment Medical Testing* 3 which states:

- it [the testing] relates specifically to the genuine and reasonable requirements of the job;

voluntary in nature and, as expected of an EOCV publication, do not focus on privacy considerations but rather on potential unlawful discrimination in testing. The International Labour Office has also released guidelines on medical testing which are non-binding in nature.[179] There are some Australian industry-specific medical standards, but compliance tends to be voluntary (eg Assessing Fitness to Drive for Commercial and Private Vehicle Drivers).[180]

2.48 Medical testing may be regulated by an individual contract or a federal industrial agreement (the latter would have the force of federal law). However, such regulation is piecemeal and would be inapplicable to certain categories of workers such as job applicants.

2.49 Apart from this, the Victorian *Health Records Act 2001* does confer protections, but only regulates health information once it has been created,[181] in which case the worker's consent can allow certain protections to be circumvented.[182] The EOCV guidelines simply suggest factors that should be taken into account once the test is 'agreed' to, such as using the inherent requirements of the job as a guide to testing. Neither the Health Records Act nor the EOCV guidelines prevent the actual medical test from occurring.

2.50 There are, of course, traditional claims available to a worker/job applicant where courts have provided remedies for breaches of certain rights relating to the worker and testing practices. These apply to all other forms of testing, and include

---

- the specific physical capacities required for the job are accurately identified and reasonable in all the circumstances;
- reasonable ways of accommodating people with disabilities/impairments have been considered;
- any facilities or services reasonably required by applicants with disabilities/impairments are provided if reasonable;
- any assessment of a person's ability to perform the inherent requirements of the job is made in conjunction with these facilities or services;
- the test only assesses current health status and does not attempt to predict any future deterioration unless the employer can demonstrate that it is reasonable to do so.

179 See International Labour Office, *Technical and Ethical Guidelines for Workers' Health Surveillance* (1998) 4–5. Interestingly, the United States has passed legislation providing additional rights to workers in this context such as the right to an independent medical evaluation in cases of disqualification, and more onerous security measures for information records: *'USA: Providing Protection with Legislation'* (2004) PersonnelToday .

180 We were informed by VicRoads (19/8/04) that the Assessing Fitness to Drive for Commercial and Private Vehicles Standard is not compulsory in nature but is treated as a 'guideline'.

181 See *Health Records Act 2001* s 1, pt 3 which refer to the regulation of 'health information'.

182 Ibid Health Privacy Principles 1 and 2.2.

actions for battery, assault, trespass to goods and breach of confidence. As raised in paragraph 2.40, medical testing may also be limited by the employer's implied duty of trust and confidence, though the parameters of the duty remain fact-driven and uncertain.[183] As Australia does not have an established right of action for breaches to privacy,[184] the law tends to indirectly capture the 'effects' of such breaches.[185] The significant time, expense and delay involved in initiating such proceedings, not to mention the almost irrevocable damage to the relationship between the job applicant/worker and employer, makes such claims uncommon and untenable for most workers.

## PSYCHOLOGICAL TESTING

2.51 *The Age* recently reported that more than 100 Australian companies use psychometric testing and that such tests are no longer confined to the white-collar workforce as blue-collar jobs become increasingly sophisticated.[186] A survey of 230 human resources decision makers in the public and private sectors, undertaken by a psychological test provider, revealed that 60% of organisations used psychological testing.[187] Such trends indicate that a growing number of employers perceive such testing to be 'a valuable, legally and ethically defensible tool' for selection decisions and assessment.[188]

2.52 The circumstances in which an employer could compel an employee to undertake a psychological test are discussed in paragraph 2.40.[189] Consultations

183 Bliss, n 156. See also para 2.40 and Chapter 3 paras 3.57–3.59 for a detailed discussion of the duty of implied trust and confidence.

184 See *Giller v Procopets* [2004] VSC 113 (7 April 2004) at paras 187–189 and *Kalaba v Commonwealth of Australia* [2004] FCA 763 (8 June 2004) at para 6. But see also *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 63 HCA [119] para 107 which arguably leaves the question of a test for privacy open to be developed, and *Grosse v Purvis* [2003] QDC [151] which at para 471 awarded damages for the invasion of privacy.

185 Traditionally, the courts have provided remedies for breaches of certain rights in relation to an individual's body and his or her property. These include actions for battery, assault, trespass to goods, and breach of confidence—for a detailed explanation see the Issues Paper, para 4.20.

186 Paul Robinson, 'Workplace Psych Tests Widen', *The Age* 18 March 2004.

187 Consultation 2.

188 Australian Psychological Society, *Comments for Victorian Law Reform Commission's Psychological Testing Technical Consultation Group* (2003) 6.

189 See Medical Testing, para 2.40, for discussion of the circumstances in which an employer could require an employee to undertake a psychological test. The APS advise us that, like medical testing, where a testee objects it is unlikely that the psychologist would proceed with the assessment: Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

reveal in practice psychological testing often occurs in a variety of contexts. This includes in the recruitment phase, as a tool to evaluate the performance or potential of existing workers (ie a 'team-building exercise') or for the purposes of promotion or reallocation of personnel.[190] There is also an emerging market in 'coaching' and 'career management' and in the provision of counselling services to workers which may involve tests of this kind.[191] 'Health counselling' is another rapidly growing area that involves use of 'behavioural health' counsellors—all of which can encompass aspects of psychological testing.[192] While not strictly speaking a psychological assessment tool, it is reported that some employers are even using lie detectors as a form of technology that tests a worker's honesty and integrity.[193]

### *WHAT IS PSYCHOLOGICAL TESTING?*

2.53 The testing process in personnel selection and assessment usually involves the employer identifying relevant 'knowledge, skills, abilities and other attributes' (the criteria).[194] Having identified the criteria, selection techniques are adopted that will help 'predict' how individuals will perform/behave against the criteria.[195] These techniques should be 'reliable' (with proven consistency over time),[196] 'valid' (relevant to and a predictor of performance)[197] and 'fair' (the same for different types or sub-groups of people within the population).[198] Despite the critical importance of such validation and reliability processes in selection testing, we were informed that there is no requirement that makes them mandatory.[199]

190 Consultation 2.

191 Consultation 2.

192 Consultation 2.

193 Wayne Howell, 'Lie Detector Boom', *The Herald Sun* (Melbourne) 26 July 2004 15.

194 Mark Davis, 'Employment Selection Tests and Indirect Discrimination: The American Experience and Its Lessons for Australia' (1996) 9 *Australian Journal of Labour Law* 187 189.

195 Ibid 191.

196 Ibid.

197 Nick Carter, Principal Consultant (Product)—SHL Australia, Consultation (21/06/04).

198 See Davis, n 194, 191. See APS, n 188, 3 which states that the technical criteria is used to assess the quality of the test including judging the adequacy of the selected conceptual framework, assessing how the test is designed, how relevant the content of the test is as well as the test's reliability and validity.

199 Consultation 2.

### *TYPES OF TESTS*

2.54 There are many different types of testing that are loosely covered by the umbrella of 'psychological testing'.[200] In the context of work, such tests are better characterised as selection tests and fall into two broad categories—aptitude/ability tests and personality/attribute tests.[201]

#### Aptitude or Ability Tests

2.55 The first type of test measures 'knowledge, skills and abilities'.[202] These are often described as aptitude or ability tests and are typically designed to measure 'general cognitive or physical abilities, although some measure more job-specific knowledge'.[203] Examples of such tests include intelligence and mental ability tests, specific job related ability tests (eg typing and word-processing skills),[204] work sample tests (when candidates are tested on a sample of actual work performed)[205] and tests of actual physical ability.[206]

#### Personality or Attribute Tests

2.56 The second category of tests are those used to measure the personal attributes or characteristics of a worker.[207] The use of such tests stems from a 'variety of theories which suggest that people's personality traits and even their general disposition towards life'[208] can assist in assessing their suitability to work in particular jobs. Unlike the first type of test, the second type does not test ability but identifies 'personality traits' and 'disposition' which can also be used to identify qualities thought to be undesirable in workers (eg dishonesty).[209]

---

200 See Carter, n 197 who states that where the term 'psychometric testing' is used, this can include ability and aptitude tests as well as personality questionnaires and career interest inventories.

201 See Davis, n 194, 189.

202 Davis, n 194, 189–90.

203 Ibid 190.

204 Davis, n 194, 190.

205 It is the APS view that work sample tests are not normally regarded as psychological tests although psychologists are often engaged by employers to provide advice about how to construct, administer, interpret and use such tests: Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

206 Davis, n 194, 190.

207 Ibid.

208 Ibid.

209 Ibid.

2.57 Some commentators argue that personality tests do not determine whether a person's personality is good or bad[210] but infer traits or tendencies to an individual.[211] Yet ultimately, it is left to the employer to decide what relevance that aspect of the personality has to the position in question (such as in assessing 'cultural fit').[212] The results 'do not provide conclusive evidence as to an individual's personality' but simply provide an opportunity for the employer to 'probe further'.[213] In fact, the place of personality tests as part of personnel selection is the source of much professional disagreement within the psychological testing industry.[214] For example, it remains in dispute whether 'honesty' as an attribute is a personality trait or a subjective social judgment of behaviour that is heavily influenced by circumstances.[215]

2.58 No matter how accurately either of these tests measure the criteria, the result will not be a valid predictor if it is based on criteria unrelated to the job.[216] Our consultations revealed that for both types of test the practice varies markedly between companies, although audits on the 'inherent requirements of the position' are gradually becoming more sophisticated.[217]

2.59 In addition, it is not feasible to have an individual test tailored specifically to one particular job in one particular organisation—it can only be tailored so far as at a certain point tests will be generalised.[218] This is the reason certain practitioners advocate a 'battery of tests' approach, the analysis of which should be undertaken not by the employer but a psychologist.[219] Again, we were advised that

---

210 Dave Griffiths, *'Psychometric Testing in Recruitment'* Nelson Griffiths 1.

211 Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04). The APS makes the point that where such tests are properly constructed, these identified 'traits' are usually supported by evidence arising from the testing of large numbers of people, and subjecting that data to complex statistical analysis.

212 Griffiths, n 210, 1.

213 Paul Lyons, 'Mind a Test?—Psychometric Tests and Personnel Selection' (1990) 61 (4) *Charter* 30 31.

214 Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

215 Consultation 2.

216 Davis, n 194, 191.

217 See consultation 2 and APS, n 188, 5. Also see Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04) who raises the concern of validity (see para 2.53) and whether, without proper reference to the inherent requirements of the position, the test can actually measure what it purports to measure.

218 APS, n 188, 6.

219 APS, n 188, 6.

there is no legal obligation that compels either the 'battery of tests' approach or use of a psychologist.[220]

### *THE PROCESS OF PSYCHOLOGICAL TESTING*

2.60 Once the content of the criteria has been determined, and the test type is selected, the actual process of testing the individual begins.

## Consent and Confidentiality

2.61 Consultations revealed that the test administrator (who can be the employer, a consultant psychologist or a recruiter) should seek written and informed consent from the person tested (the testee) which in practice tends to be a general rather than specific consent.[221] APS ethical guidelines[222] exist which require testers to avoid using the test to the 'disadvantage of the testee' and permits a report of the test to be prepared for both the employer and the employee.[223] There is an ethical guideline to give feedback to the testee, but we were informed that this does not always occur.[224] The guidelines also require that any decision made on the basis of test results should be undertaken confidentially.[225] The APS ethical guidelines provide assistance to psychologists who are APS members, despite non-psychologists having access to test results and reports.[226] Similarly, the Victorian Psychologists Registration Board's code of behaviour is designed to apply only to registered psychologists.[227] Neither the code nor the APS guidelines require mandatory compliance.

---

220 Consultation 2.

221 Consultation 2.

222 For detail see Ian Kendall, Jo Jenkinson, Molly de Lemos et al, *Supplement to Guidelines for the Use of Psychological Tests* (1997).

223 Consultation 2.

224 Consultation 2.

225 Ibid.

226 According to the APS, compliance by members with these guidelines is expected but not strictly mandatory. Failure to comply may be used as a ground for disciplinary action but is not automatically unethical. The guidelines contemplate unusual circumstances that may justify departure from the guidelines (though such departure has to be professionally defensible): Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

227 See *'Code of Behaviour for Psychologists'* (1997) Psychologists Registration Board of Victoria which is a recommended code of behaviour for registered psychologists (the Board's ability to investigate complaints is limited to registered psychologists, see Part 3 of the *Psychologists Registration Act 2000*).

## Availability of Tests

2.62 Consultations indicate that test availability is controlled either by the test publishers and distributors[228] (presumably in accordance with their own ethical, professional and/or commercial imperatives) or not at all. It seems practices vary widely, ranging from tests that are provided through a trained consultant, to tests that are simply downloaded from the Internet.[229] Based on our consultations, there seemed to be no real standardisation or regulation as to availability of these tests.[230]

## Administration of Tests

2.63 During consultations, the Australian Psychological Society (APS) suggested group tests might be administered by a trained assistant under the psychologist's professional supervision.[231] However, the APS' view is that individual psychological tests required personal administration by a psychologist.[232] Despite this, we were informed there is no legal requirement within the industry compelling this practice.

## Interpretation of Tests

2.64 The general view expressed in consultations was that psychologists should interpret tests.[233] We were advised that when a test is sold to an employer there is generally a 'goodwill' understanding that the psychologist will be retained to interpret the test results.[234] There are courses which train company personnel in the interpretation of test data, but the value of this can be lost where there is staff turnover.[235] However, provision of test analysis training is not necessarily contingent on the sale of a test, nor is it compulsory in any other way.[236]

2.65 Interestingly, one commentator takes this point further and argues that a general psychological degree may not even be enough, with psychologists per se

228 Consultation 2.

229 Consultation 2.

230 Consultation 2.

231 APS, n 188, 5.

232 See Consultation 2 and APS, n 188, 5.

233 Consultation 2.

234 Consultation 2.

235 Ibid.

236 Ibid.

lacking the necessary skills to determine and interpret tests.[237] The author proposes a specialisation within psychology, where 'it is professional judgement that determines whether a test has been properly used, and only the professional with a full knowledge of the context and purpose of testing can make this judgement'.[238]

## Storage and Disclosure of Test Results

2.66 Our consultations revealed employers and psychologists are generally uncertain about how to store test results and no consistent practice exists.[239] The APS has voluntary guidelines stating that psychologists must maintain control over psychological records.[240] We were also advised that psychologists have a practice of seeking written and informed consent from the testee with respect to disclosure of test results.[241] As discussed in paragraph 2.61, these ethical obligations would obviously not apply to non-psychologist test administrators.

2.67 Consultations also revealed that the question often asked by the psychologist in this context is 'who is the client?' The answer to this could also govern the subsequent storage and disclosure of reports.[242] We were advised that in the workplace context, as the client is nearly always the employer, issues concerning third party disclosure were usually resolved according to the employer's wishes.[243] For example, one test provider cited instances where a pre-existing stress condition revealed in a pre-employment psychological test may be disclosed to the employer if it is considered relevant to the risk of a future WorkCover claim.[244]

---

237 Jo Jenkinson, 'The Skill Basis of Psychological Testing' (1991) 4 (1) *Psychological Test Bulletin* 5 6.

238 Ibid 11.

239 Consultations 2, 10.

240 The APS informed us that these guidelines incorporate federal and state information privacy requirements: Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

241 Consultation 2. See also Code of Behaviour for Psychologists, n 227 which states that psychologists must ensure 'appropriate confidentiality in storing, transferring and disposing of all records under their control'.

242 Ibid.

243 Ibid.

244 Ibid. Depending on the nature of the consent given, this practice may breach both the provisions of Health Privacy Principle 2 in the *Health Records Act 2001* which deals with use and disclosure of health information, and the National Privacy Principle 2 in the *Privacy Act 1988* (Cth) which deals with use and disclosure of personal information.

### *REGULATION*

2.68 We were advised that while many test distributors observe 'conventional test development standards', a significant number of tests on the market are not adequately developed or validated.[245] The quality of tests seemed to be largely left to the market to judge.[246] Our consultations revealed approximately 40% of tests are administered by non-psychologists and it is likely that standards have deteriorated as a result.[247]

2.69 We were informed that employers can also enter into a leasing arrangement with test providers where they may download personality/aptitude tests from the Internet, subject to any applicable contractual requirements.[248]

2.70 Providers sometimes refuse to sell tests and in this sense they are self-regulatory.[249] We were advised that no formal accreditation is needed to administer psychological tests.[250] The APS issues ethical guidelines and deals with certain complaints against member psychologists. A breach of these guidelines can result in disciplinary action, but membership of the APS is voluntary.[251] Most professional misconduct complaints are referred to the Psychologists Registration Board—the state's regulatory authority. However, the jurisdiction of the board is limited to investigations into 'registered psychologists'.[252] This does not cover many kinds of psychological test providers which, as consultation revealed, can often include non-psychologists.[253] Additionally, the board's code of behaviour is not compulsory, but is instead designed to 'assist' psychologists.[254]

2.71 Interestingly, apart from the APS, there was little discussion of the collection, access, storage and disclosure requirements contained in the Health Records Act in the context of psychological testing. This may indicate that test providers are either unaware of the requirements, or do not generally consider that

245 Consultation 2.

246 Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

247 Consultation 2.

248 Consultation 2.

249 Consultation 2.

250 Arthur Crook, Principal Policy Analyst—Australian Psychological Society, Consultation (5/8/04).

251 Consultation 2.

252 See Part 3 of the *Psychologists Registration Act 2000*. See also Part 5, s 61 which provides for an offence relating to a person claiming to be a psychologist, or a registered psychologist, when they are not.

253 Consultation 2.

254 See Code n 227.

information gained from such selection tests contain information about 'psychological health'.[255] Arguably, psychological health may include assessments on intelligence, or even indirectly reflect an intellectual disability or personality disorder (eg a finding that a person is 'not a team-player' may be as a result of an anti-social disorder or disability). If these assessments were used to unlawfully discriminate against a worker, reactive anti-discrimination laws would apply.[256] However, the possible protection that may be conferred on a worker under the Health Records Act remains unclear in the context of certain types of psychological testing.

## ALCOHOL AND DRUG TESTING

### *TYPES OF PRACTICES*

2.72 We were informed during consultations that urine testing is the most common form of alcohol and drug testing. It reveals the presence of these substances within a limited time frame[257] where the window of detection varies between individuals, often depending on the rate of metabolism, but other factors may be relevant (eg frequency of use, the type of drug, the presence of disease etc).[258] In addition, certain people from particular cultures can have more dilute urine[259] which disproportionately decreases the likelihood of a positive test. This may raise the possibility of potential unlawful discrimination.[260] An Australian

255 See the *Health Records Act 2001* s 3 which states that 'health information' means (a) information or an opinion about—(i) the physical, mental or psychological health (at any time) of an individual.

256 See n 156. It should be noted that not only direct discrimination (eg section 8 of the *Equal Opportunity Act 1995*) but 'indirect discrimination' could also apply in this context. See for example section 9 of the *Equal Opportunity Act 1995* which states that indirect discrimination occurs if a person imposes, or proposes to impose, a requirement, condition or practice (a) that someone with an attribute does not or cannot comply with; and (b) that a higher proportion of people without that attribute, or with a different attribute, do or can comply with; and (c) that is not reasonable. Where an apparently neutral psychological test indirectly discriminates against people with certain types of personality disorders, this may result in unlawful discrimination on the basis of disability (see also section 6 of the federal *Disability Discrimination Act 1992*).

257 Consultation 9.

258 Ibid.

259 Dilute urine reduces the chance of detection. Concentrated urine (which can for example, occur if dehydrated or with renal dysfunction) will increase the chance of drug detection: Adjunct Professor Olaf Drummer, Head Scientific Services—Victorian Institute for Forensic Medicine, Consultation (18/6/04).

260 See Equal Opportunity Act, n 256.

Standard[261] (the Standard) has been developed with respect to urine testing in identifying specific drug groups, providing recommended cut-off levels for measuring the presence of these drugs as well as detailing collection procedures. Urine testing for drugs is the only form of testing that is covered by an Australian Standard.[262]

2.73 Blood testing can also be used to detect drugs and alcohol, however, it is not commonly used because of its highly invasive nature.[263] Blood testing is good at determining recency of drug and alcohol use, and it is easier to interpret the likely physiological and pharmacological effects of such use from blood samples.[264]

2.74 We were informed that breath testing is predominantly used for detecting the presence of alcohol.[265] As stated, there is no equivalent Australian Standard on breath testing, with cut-off levels tending in practice to default to the general .05 driving impairment cut-off level.[266] Our consultations revealed this alcohol testing/breathalyser process seemed to be generally accepted by both management and unions/workers.[267] Even so, breathalysers are of varying standard and require constant maintenance.[268] Alcohol breathalysing is a very precise process, second only to blood alcohol testing in precision.[269] However, not many laboratories are set up to conduct a blood alcohol test. We were advised that where this occurs, it is highly desirable that samples be processed by a National Association of Testing Authorities (NATA) accredited laboratory.[270]

---

261 Standards Australia/Standards New Zealand, *Procedures for the Collection, Detection and Quantitation of Drugs of Abuse in Urine* AS/NZS 4308:2001 (2001).

262 We have been informed that a new Standards Australia committee has been convened to look into a standard for oral fluid: Adjunct Professor Olaf Drummer, Head Scientific Services—Victorian Institute for Forensic Medicine, Consultation (18/6/04).

263 International Labour Office, *Management of Alcohol- and Drug-Related Issues in the Workplace* An ILO Code of Practice (1996) 37.

264 Adjunct Professor Olaf Drummer, Head Scientific Services—Victorian Institute for Forensic Medicine, Consultation (18/6/04).

265 Consultation 9.

266 Ibid. Note that a zero limit applies to probationary and commercial drivers.

267 Ibid.

268 Ibid.

269 Ibid. See also Adjunct Professor Olaf Drummer, Head Scientific Services—Victorian Institute for Forensic Medicine, Consultation (18/6/04).

270 Ibid.

2.75 Consultations revealed a growing trend towards the use of saliva testing for alcohol and drugs.[271] This is considered a less invasive method than urine testing as the process simply involves taking a swab.[272] We were informed that saliva tests have a shorter detection window[273] but again, unlike urine testing, they are not covered by an Australian Standard. Sweat testing is another possible method, and generally approximates the process of saliva testing. It is a relatively new form of test and little data is available on usage.[274]

2.76 We were informed that there is significant use of hair testing in the US and UK in the pre-employment context.[275] It was indicated that this is considered a reliable test in detecting the 'presence' of alcohol metabolites and drugs, and the detection window can be many months. However, it is expensive and labour intensive and can also have a racially differential impact (eg black hair retains the presence of alcohol/drugs for longer),[276] raising potential issues of unlawful discrimination.

2.77 Generally speaking, there are three approaches to drug-testing:

- use do-it-yourself kits;
- send results to a non-accredited laboratory; or
- send results to a NATA accredited laboratory.[277]

### *PROCESSES OF TESTING*

2.78 The circumstances in which an employer could compel an existing employee to undertake a drug and alcohol test are discussed in paragraph 2.40. As for the actual process, the Standard details the collection process for urine testing which is summarised below. However, we are advised there is no general standardisation of process for other forms of testing and they remain almost entirely unregulated.[278]

---

271 Ibid.

272 Ibid.

273 Ibid.

274 See ILO report, n 263, 37.

275 Consultation 9.

276 Consultation 9.

277 Ibid.

278 If a laboratory seeks accreditation by NATA (and there is nothing compelling accreditation), NATA conducts detailed inspections of process on technical, safety and security grounds. However, we were

2.79 The Standard prescribes the process of urine testing in two stages. The first stage is the screening test or the processing of the initial sample which can be undertaken by a laboratory or company personnel. This should then be sent to a laboratory for a confirmatory test (second stage),[279] though there is nothing which legally compels this second test.[280] We were informed that the samples may be linked to the testee or de-identified, depending on what the employer requires.[281] Consultations revealed that the process of alcohol and drug testing in the workplace is most likely to be contained in a company policy[282] or where applicable a federal industrial agreement,[283] with considerable variation in process existing between companies.[284]

## Range of Testing

2.80 A report by the United Nations identified the range of testing that can be carried out in the workplace including:

- pre-employment testing;
- probable cause testing;[285]
- reasonable suspicion testing;[286]

---

informed by NATA that the accreditation criteria does not focus on legislative compliance with, for example, the *Health Records Act 2001* (Vic), but rather focuses on a 'technical competency review' (in accordance with International Standard 17025 General Requirements for the Compliance of Testing and Calibration Laboratories): Maritta Purcell, Manager Forensic Science Laboratory Accreditation Program—NATA, Consultation (10/8/04). As such, compliance with the requirements of the Health Records Act would not form part of this type of review.

279 Australian Standard, n 261, 17–18.

280 Consultation 9.

281 Consultation 4.

282 Ibid.

283 Consultation 4. Note that a federal industrial agreement can be either a collective certified agreement or an individual AWA.

284 Consultation 9.

285 'Probable cause' is a legal term used in most common law American criminal law jurisdictions that denotes the standard by which a police officer may conduct a personal or property search, or an arrest. This term comes from the Fourth Amendment of the United States Constitution. A number of definitions exist. Arguably the most widely held definition is 'a reasonable belief that a crime has been committed'. However, this definition is controversial. A proposed alternate definition is 'reason to believe that an injury had criminal cause' see *'Probable Cause'* Word iQ .

286 In Australia, finding a 'reasonable suspicion' has been considered in cases as meaning 'there must be reasonable grounds for the relevant state of mind and the existence of facts which are sufficient to induce such': *R v Chan* (1992) 28 NSWLR 421 at 437. 'Suspicion' carries 'less conviction than 'belief': *Tucs v Manley* (1985) 62 ALR 460 at 461. 'To say that a suspicion is reasonable does not

- periodic testing;
- random testing;
- testing on return from treatment;
- testing related to transfer or promotion; and
- voluntary testing.[287]

## Consent to Testing

2.81 With urine testing, the Standard does not require that the written consent of the testee be sought prior to the commencement of testing. The Standard simply requires that the testee certify in writing ownership of the sample prior to it being sent to the laboratory.[288]

2.82 We were informed that if consent is sought in the pre-employment/ engagement context, it is more likely to be verbal rather than written.[289] As discussed in paragraph 2.40, current employees may consent to be tested (in their contract or otherwise).[290] Once the test has been conducted, consultations suggest that the process would then most likely be governed contractually between the employer and the laboratory, rather than between the testee and the laboratory.[291]

## Collection/Storage of Test Samples

2.83 In accordance with the Standard, the process of collection involves the use of a sealed/tamper-proof bottle (which is sealed in the presence of the testee)

---

necessarily imply that it is well-founded, or that the grounds for suspicion must be factually correct': *Tucs v Manley* at 461.

In the United States 'reasonable suspicion' can mean requiring an officer to be able to 'articulate facts' constituting a minimal level of objective justification. This is usually distinct from 'probable cause' which requires greater certainty in using a reasonable person's standard of proof in order to justify actions. This is defined by the facts and circumstances within the officers' knowledge and of which they had reasonably trustworthy information sufficient to warrant a reasonable person believing an offence had or was being committed. See Levels of Proof Instructions at *'Levels of Proof Instructions'* National College of DUI Defense, Inc .

287 J Mrland, *'Types of Drug-Testing Programmes in the Workplace'* (1993) United Nations: Office on Drugs and Crime 4.

288 Australian Standard, n 237, para 3.3.4(c).

289 Consultation 9.

290 See para 2.40 for a detailed explanation of when and how an employer can require an employee to undertake a test. See also paras 3.60–3.68 for problems with workers providing genuine consent within the work relationship.

291 Consultation 9.

provided to an accredited laboratory with a verifiable chain of custody.[292] The Standard also sets out a transportation process which is intended to minimise possible contamination.[293] The testee should be satisfied that the sample has not been tampered with.[294]

2.84 We were advised that the employer is expected to protect the sample and decide how it is stored.[295] With urine, for example, we were told that in the workplace context there is no law regarding how long samples should be kept.[296] The Standard suggests a period of one-year storage for positive samples, but otherwise samples are stored and disposed of 'in accordance with laboratory policy'.[297] Additionally, we were informed that employers and laboratories do not usually have sufficient storage facilities, which results in samples being outsourced to a third party storage facility.[298]

### Testing Cut-off Levels

2.85 The Standard on urine testing does not prescribe cut-off levels for impairment, but rather tests for the 'presence' of drugs.[299] In this way, it does not distinguish between drug use and abuse, nor impairment.[300] We were informed that cut-off levels applied to drug testing can vary and there is no one standard that regulates all drug test results.[301] The Standard relates only to urine testing and compliance with it is entirely voluntary.

---

292 Australian Standard, n 261, 12.

293 Ibid.

294 Consultation 9.

295 Ibid.

296 Consultation 9.

297 Australian Standard, n 261, 13.

298 Consultation 9.

299 Australian Standard, n 261, 15–16. See also Lewis Maltby, *Drug Testing: A Bad Investment* (1999) 9, 19 for discussion of the difference between presence of drugs and impairment by drugs, and distinguishing between use and abuse of drugs.

300 Behrouz Shahandeh and Joannah Caborn, 'Ethical Issues in Workplace Drug Testing in Europe' (Paper presented at the Seminar on Ethics, Professional Standards and Drug Addiction, 6–7 February 2003, Strasbourg) 8.

301 The cut-offs also vary with those of the US, UK and EU, at least for some analyses, which is a current issue of contention in 'harmonising' the standard: Adjunct Professor Olaf Drummer, Head Scientific Services—Victorian Institute for Forensic Medicine, Consultation (18/6/04).

2.86 There has been little debate over alcohol cut-off levels which measure impairment in a work context. Consultations reveal that presently, cut-off levels established for impairment in driving (eg .05) are relied on and these have been found to be legally defensible.[302] Our technical consultation group recommended that if impairment were an issue, a medical professional (as opposed to laboratory staff) would be required to assess impairment.[303] However, there seems to be nothing requiring this practice.

## What is Tested For?

2.87 With urine testing, the Australian Standard lists standard drug groups for testing purposes. These include:

- opiates (eg heroin, methadone);
- sympathomimetic amines (eg speed, diet pills);
- cannabis metabolites (marijuana);
- cocaine metabolites (cocaine); and
- benzodiazepines (eg valium, serapax, rohypnol).[304]

2.88 This is only a suggested list, and there is no real limitation on an employer testing for other types of drugs, if required. This may result in testing for drugs that are not relevant to the inherent requirements of the job (and as such increasing the possibility of unlawful discrimination occurring).[305] An additional question remains regarding testing for over-the-counter/prescription drugs and their abuse. Examples of these include benzodiazepines (valium, serapax), opiates such as codeine and stimulants like pseudoephedrines.[306] It cannot be presumed that all drug use involves illegal drugs. We were informed that one of the most widely abused categories of drugs are therapeutic drugs (eg anti-depressants), the abuse of which can leave a worker impaired.[307]

302 Consultation 9.

303 Ibid.

304 Australian Standard, n 261, 16.

305 See para 2.47 for Equal Opportunity Commission of Victoria guidelines on medical testing.

306 Consultation 9.

307 Ibid.

## Use and Disclosure of Information

2.89 All manner of assumptions can be imputed[308] from test results (such as disability, pregnancy and sexuality).[309] There are no restrictions on the use and disclosure of such information other than what may be provided by health privacy and discrimination law requirements.[310] It is another question whether or not employers/laboratories adhere to these requirements. Our consultations revealed the provisions of the Health Records Act were generally not being followed when it came to information gained from alcohol and drug testing.[311]

### *REGULATION*

2.90 There is no consistent, comprehensive regulation of the practice of alcohol and drug testing in Australia. It is randomly regulated through specific regulations in particular industries,[312] in some federal industrial agreements[313] or in company policies.[314]

2.91 In the context of drug and alcohol testing, the Health Records Act was not raised during consultations or in submissions received by the Commission. It may be unclear whether the provisions of the Act apply to these tests. Ultimately, it

---

308 'Imputed attributes' are covered by anti-discrimination laws. For example see section 7(c) and (d) of the *Equal Opportunity Act 1995* (Vic) which defines discrimination to include 'a characteristic that is generally imputed to a person with that attribute' and 'that a person is presumed to have that attribute or to have had it at any time'. Note that federal anti-discrimination provisions also exist to this effect.

309 See Equal Opportunity Act n 158.

310 Ibid.

311 Consultations 9, 10, 11.

312 For example see Western Australia's *Mine Safety and Inspection Regulations 1995*, specifically regulation 4.7(1) states:

'A person (whether or not an employee) must not be in or on any mine while the person is adversely affected by intoxicating liquor or drugs. Penalty: see regulation 17.1. Regulation 4.7(4) states that a person must not, without the knowledge and permission of the manager of the mine:

(a) have any intoxicating liquor or deleterious drug in his or her possession in or on a mine; or

(b) consume any intoxicating liquor or deleterious drug while in or on a mine'.

313 See the Construction, Forestry, Mining and Energy Union and James C and Simon Ball (AG2003/8097) (James C & Simon Ball and CFMEU Building and Construction Industry Collective Bargaining Agreement 2002–2005) for an example of an agreement that uses the CFMEU's Alcohol & Other Drugs Policy, which is included in the majority of agreements across the construction industry.

314 See Bliss n 156.

depends on whether or not these processes collect health information. 'Health information' is defined as information or an opinion about the physical or mental 'health' of an individual.[315] 'Health' is not defined by the Act, but *The Macquarie Dictionary* defines it to include '1. soundness of body…2. the general condition of the body or mind with reference to soundness and vigour'.[316] In accordance with this definition, it is arguable that information gained from alcohol and drug testing processes could be captured by the provisions of the Act. However, in practice, the application of the Act in this context remains unclear, and as the Act only applies to 'information', it does not prevent the actual introduction of the alcohol and drug testing process into the workplace. Similarly, anti-discrimination laws are reactive and do not prevent the practice being introduced (see paragraph 2.49).

2.92 Apart from this, employers can choose to follow the Standard on urine testing, but there is no legal requirement to do so. All the other forms of testing described above do not possess an equivalent Australian Standard. A voluntary accreditation practice exists as a form of self-regulation where NATA can recommend de-accreditation if a member laboratory fails to improve its standards.[317] However, the parameters of NATA's assessments focus on reviewing technical competency[318] and its powers are restricted to controlling the NATA accreditation status of its members, and membership is voluntary.[319]

## CONCLUSION

The overview of these practices reveals the quite extraordinary technological developments that are integral to their use. In what are largely under- or un-regulated areas, these developments and innovations seem to be driving and determining the use of such practices, despite the existence of other important considerations such as proportionality and reliability. Chapter 3 will explore these issues in identifying possible gaps in protection from both employer and worker perspectives.

315 *Health Records Act 2001* (Vic) s 3(1).

316 A Delbridge, JRL Bernard, D Blair et al (ed) *The Macquarie Dictionary* (3rd ed) (1997) 986.

317 Consultation 9.

318 See Purcell, n 278.

319 Ibid. Marrita Purcell, Manager–Forensic Science (Laboratory Accreditation Program, NATA), Consultation (19/8/04).

# Chapter 3
# Gaps in Protection

## INTRODUCTION

3.1 In our Issues Paper, we identified and outlined the legal gaps in the protection of workers' privacy.[320] We then met with employers and employees during our consultation process to explore these gaps in relation to surveillance, monitoring and testing practices (see Chapter 1). We undertook research and consultations to describe the processes involved in these particular practices, including the existing legislative and self-regulatory regimes (see Chapter 2).

3.2 In this chapter we critically examine the issues from the perspective of employers, workers and third parties in the workplace.

3.3 We begin by outlining how privacy issues are affected by the nature of the work. We critically review the arguments employers use to justify the use of workplace surveillance, monitoring and testing. We then look at issues from the workers' perspective. The final section considers third parties who might be affected by these practices, and how the privacy rights of third parties might also affect the privacy rights of workers. Underlying all three perspectives are the perceptions of employers, workers and third parties of just how far the parameters of the 'work relationship' extend.

3.4 We confine the comments that follow to the implementation and use of surveillance, monitoring and testing in the workplace. Discussion does not extend to the wider issue of regulating other parties involved in these practices (such as suppliers of surveillance technologies, laboratories involved in drug and alcohol

320 See Appendix 5 and Appendix 6 which summarise the coverage and limits of privacy laws and relevant workplace relations laws respectively.

testing, the medical profession or psychologists) as this is beyond our terms of reference.

## THE NATURE OF THE WORK RELATIONSHIP

3.5 Within Australian workplaces there are many different types of work relationships including employment, independent contracting and voluntary work. As we explained in paragraph 1.4, all of these relationships are covered by our terms of reference. The ambit of the work relationship can extend to cover multiple workplaces and certain after hours activities, as well as the pre- and post-employment contexts. Apart from the formal work contract, workers' rights and obligations can arise from a number of external sources including legislation, common law (express and implied), equitable principles, industry practice and terms in awards and collective agreements.[321]

3.6 The primary source of privacy rights in Australia is legislation which focuses on consumer rights and information privacy. But the contractual relationship that exists between suppliers and consumers differs markedly from the relationship between workers and employers. This is largely because a feature of the work relationship is the 'control' the employer exercises over the worker. This notion of control does not exist within the consumer relationship.[322]

3.7 The worker 'brings to the work relationship their only asset, namely the capacity to perform work'.[323] The employers' priority is to maximise the return on their investment in accordance with market forces.[324] To this end, the employer must be able to exert necessary control over their workforce. The exertion of control varies, depending on the type of worker. For example, one of a number of factors that distinguish an employee from an independent contractor is the expectation that an employer will exert a greater degree of control over an employee.[325] The employers' right and ability to exert control over their workers is mediated through the various sources of legal rights and obligations noted in paragraph 3.5.

---

321 Creighton and Stewart, n18, 221–33.

322 Ibid, 208–13.

323 Ibid, 8.

324 'Which can mean maintaining, increasing or reducing production and labour force, the ability to innovate in terms of product and work methods, as well as the right to transfer ownership or relocate the business': Ibid, 9.

325 Ibid, 201–20.

3.8 These issues and obligations that arise within the work relationship will be examined from both the employers' and workers' perspectives.

## EMPLOYER PERSPECTIVES

3.9 Businesses face an increasingly competitive and complex environment. Employers argue that they should be free to manage their enterprises as efficiently as possible and to defend themselves against potential legal claims. The latter issue has become a hot topic in light of recent corporate collapses and an increased emphasis on corporate governance issues.[326] In addition, the increasing globalisation of companies has an impact on Australian operations where overseas corporate headquarters may apply policies without much local adaptation.[327]

3.10 Employers argue that surveillance, monitoring and testing may be necessary for a range of reasons including:

- protection of property and control of computer equipment;
- selection of workers and measurement of their performance and productivity;
- reduction of the risk of legal liability;
- gathering of evidence relevant to legal issues; and
- maintenance of security.

3.11 During our consultations, employers also expressed concerns about the lack of certainty in the current regime. This includes inconsistencies between the various state and federal regulations that apply to businesses.

3.12 In this section we critically examine the reasons why employers use surveillance, monitoring and testing in the workplace, along with their concerns about regulatory uncertainty.

---

326 See for example, the requirements of the ASX Corporate Governance Council, *Principles of Good Corporate Governance and Best Practice Recommendations* (2003).

327 This can have particular impact where in countries like the United States, psychological and alcohol and drug testing are commonly used in the selection and employment context: Maltby, n 299, 4. A more local market force is the emerging trend of tenders and licensing requirements necessitating all workers involved on the proposed project to be medically and/or drug and alcohol tested. This has the consequence of a third party client requiring an employer to establish such practices: Consultation 19.

## PROTECTION OF PROPERTY

3.13 Employers told us that video surveillance was frequently used to protect property against theft. Potential theft is a concern to any business that handles stock, cash or property, but it is a particular issue for retailers.[328] The latter argue that the use of video surveillance is necessary to combat stock losses and associated costs that result from theft.[329] They are concerned that if they are restricted in their ability to use video surveillance, particularly covert surveillance, the costs of theft in Victoria will skyrocket. They believe this has been the case in New South Wales where it is necessary to gain a magistrate's approval for covert video surveillance.[330] Employers said their use of covert video surveillance in New South Wales has markedly decreased due to the administrative costs of the approval process, and as a result they believe that theft and fraud have increased.[331] They argue that this, in turn, will lead to increased costs of consumer goods—an unintended consequence of the restriction on covert surveillance.

3.14 Australian Institute of Criminology research supports the view that retail theft is a cost to society.[332] At the same time, it indicates that as most retail theft is established by audits of stock losses rather than directly witnessed, it is not clear whether it is perpetrated by customers, staff or suppliers.[333] While surveillance may have a part to play in combating theft, it is the manner and the extent to which it is conducted in the workplace that is of concern from a privacy perspective.[334] For example, are cameras aimed at workers or are they just aimed at stock or equipment? Are workers under constant surveillance or are they able to move in and out of the range of surveillance cameras?

3.15 Employers told us they only use monitoring and surveillance if there is a clear business case to do so. One employer said covert video surveillance is only used when there is some kind of triggering event (eg if a theft occurred). It is used

328 During consultations, retail employers indicated that they believe that 40% of retail theft is by staff.

329 Consultations 5 and 17.

330 See *Workplace Video Surveillance Act 1998* (NSW) ss 3,4,7 and pt 3. This is also the case under new workplace surveillance laws proposed for New South Wales. See the exposure draft of the Workplace Surveillance Bill 2004 (NSW), particularly cls 3, 5, 8 and pt 3. See n 4 for the objects of the Bill.

331 Figures which bear out these concerns are not readily available.

332 See Diana Nelson and Santina Perrone, *Understanding and Controlling Retail Theft* (2000) 2.

333 Ibid 1.

334 The Australian Institute of Criminology argues that simply increasing security alone will not prevent retail theft. Ibid 6.

as a last resort as part of a full investigation and in accordance with strict policies and procedures.[335] Installing surveillance and monitoring equipment is costly and is not used unless the benefit outweighs the cost. Employers may factor non-economic issues such as workers' privacy interests into this equation, but our impression is that employers place paramount importance on economic factors.

## CONTROL OF EMPLOYERS' COMPUTER EQUIPMENT

3.16 Employers argue that as they own their computer equipment they have a right to control that equipment. Accordingly, they consider they have a right to use surveillance and monitoring as a means of ensuring their equipment is used appropriately.

3.17 During consultations, the issue of control of computers was discussed in relation to email and Internet monitoring. Employers argued that they have the right to view workers' emails, regardless of whether or not they are personal.[336]

3.18 It is generally accepted there will be some personal use of work computers for access to email and the Internet.[337] Email is becoming the predominant form of personal and business communication.[338] With the increasing trend by banks and other essential service providers toward the use of online access for bill payments, people are likely to become more dependent upon computers to carry out many personal daily tasks. For this reason, what is considered 'reasonable personal use' of work computers is also likely to change. This may be compounded by longer working hours, which makes it harder for people to attend to their daily tasks.

3.19 If employers are willing to accept there will be some personal use, the Commission's view is there should be respect for the privacy of a worker's computer use, unless there is cause to suggest the worker is abusing the system.

---

335 Consultation 17.

336 In discussing the control of computer systems during our consultations, we compared the reading of a worker's personal emails by an employer to the reading of a hard copy letter marked 'personal'. We asked employers where they would draw the line at reading the letter. Most of them said that they would read the letter if it was lying on someone's desk. They were less certain about it if it was in a desk drawer. All of them said they would not read it if it was in someone's handbag. There were varying opinions as to where the line should be drawn in regard to reading the letter but they were more certain about being able to access emails as they own the equipment: Consultation 7.

337 See CNIL, *Cyber-Surveillance in the Workplace: A Report presented by Mr Hubert Bouchet, Delegate Vice-Chairman of the CNIL* (2002) 11 and Consultation 7.

338 Lane, n 79, 138.

This is particularly the case since monitoring tools are not generally able to separate personal from work-related emails.[339] For example, if a worker is unproductive because of suspected overuse of personal emails, it might be more effective to measure productive output rather than to use email monitoring. If workers are using the Internet excessively, and clogging up an employer's computer system, it may be more effective to use technological constraints to block frequently used websites. A minimal amount of targeted monitoring might be used, if appropriate, to confirm suspicions about these issues.

## MANAGEMENT ISSUES

### *SURVEILLANCE AND MONITORING AS MANAGEMENT TOOLS*

3.20 Employers say they are entitled to expect that workers who have been engaged to perform a certain role will perform that role.[340] Accordingly, employers may look to surveillance and monitoring as a way of supervising workers and measuring workers' performance and productivity. For example, surveillance might be used to identify and rectify production bottlenecks in manufacturing environments.[341] Monitoring might be used to assess whether customer service workers are adequately performing their roles. But are monitoring and surveillance practices valuable tools or simply substitutes for good management?

3.21 Call centres are an example of an environment where workers are subjected to intense monitoring. A recent study of call centre work practices found work tasks are monitored, including length of call, time between calls, content of calls and politeness towards customers.[342] The results are often displayed for all workers to see. The study found there is a high level of control of workers' activities and it is not unusual for call centre workers to have to raise their hands or seek permission to use the bathroom.[343] Technological supervision is used so

339 See Chapter 2, para 2.20.

340 Victoria Police argue that when employers employ someone to perform certain actions and activities, they are entitled to know what action and activities the employee is actually performing: Submission 31.

341 It was the view of our technical consultation group that video surveillance is not generally used to assess performance: Consultation 3. One example where it can be used to assess performance is in retailing, where video footage from a store might be used to assess how security personnel handle customers: Consultation 17.

342 Diane van den Broek, *'Surveillance, Privacy and Work Intensification within Call Centres'* WorkSite 2.

343 Ibid.

extensively in the call centre industry that call centres have been described as 'electronic sweatshops'.[344]

3.22 Call centres represent an extreme position in relation to monitoring and surveillance. However, the study found it is not the use of surveillance and monitoring practices of themselves that are an issue for call centre workers, it is the way management uses these practices to intensify work by continually increasing output goals.[345] In our view the two issues are inextricably linked, as employers would not be able to collect and use such an array of information if not for the use of intensive monitoring and surveillance. Unions told us call centre workers are concerned about over monitoring and that excessive monitoring and its results can be used to bully workers.[346]

3.23 Employers told the Commission that surveillance and monitoring can be particularly helpful where workers operate in an isolated environment. In the transport industry, for instance, truck drivers work alone much of the time.[347] Trucks can be very expensive pieces of equipment[348] and employers in the transport industry have an interest in knowing where their vehicles are and how they are being used. This is important to employers, not only from a management perspective, but also to ensure they are fulfilling legal obligations relating to occupational health and safety.[349] In its submission, the Victorian Transport Authority (VTA) said that where workplaces are mobile and remote, with no direct supervision, electronic monitoring becomes an essential tool.[350] Some of the devices used can monitor driving and rest times, which the VTA said are lawful

344 Ibid. See also Julian Sempill, 'Call Centres: Total Control Made Easy' in *Case Study, Principles of Labour Law* (1999).

345 van den Broek, n 342, 4.

346 ACTU email correspondence about call monitoring anecdotes, 10 November 2003.

347 Similarly, rural employers find drug and alcohol testing particularly useful where a high proportion of employees use heavy and/or dangerous machinery in isolated areas, and employers are unable to provide direct, constant supervision: Consultation 10.

348 We were told during consultations that trucks can cost up to $400 000: Consultation 18.

349 See *Occupational Health and Safety Act 1985* s 21(1), which requires employers to provide and maintain as far as is practicable for employees a working environment that is safe and without risks to health.

350 Submission 6.

alternatives to paper-based log books.[351] The VTA said it is not so much an issue of knowing where the worker is, but knowing where the workplace is.[352]

3.24 One union representative observed there may be some justification for using surveillance for genuine security reasons, and in relation to productivity where it can be measured.[353] However, from the union's point of view, the productivity argument is becoming less justifiable as more jobs are transformed into 'thinking jobs' in which productivity is difficult to measure easily.[354]

3.25 Additionally, studies have indicated that constant surveillance and monitoring in the workplace can have negative effects.[355] Workers who have their performance technologically monitored can experience health problems such as stress, tension, anxiety, depression, fatigue, anger, headaches and musculoskeletal problems.[356] These problems can lead to lower productivity, absenteeism and high turnover.[357] One submission said constant monitoring can also have a negative effect on workplace morale, creating an atmosphere of distrust and disrespect, and intensifying the division between management and workers.[358]

3.26 Some commentators have indicated that once installed, surveillance and monitoring systems are rarely removed or scaled down.[359] This so called 'function creep' can result from a number of factors. Function creep can occur where an employer has initially invested in a video surveillance system with a centralised monitoring station.[360] In such a case, the cost of adding extra cameras and locations is relatively low.[361] Advances in technology also put pressure on

351 Submission 6.

352 Submission 6.

353 For example, whether goods were delivered on time can be measured. Productivity can also be measured in sales jobs, eg by the value of goods or services sold.

354 Consultation 12.

355 For some examples of studies, see those cited in International Labour Office, *Workers' Privacy—Part II: Monitoring and Surveillance in the Workplace* 12(1) (1993) 22–4.

356 Submission 2. See also Anna Johnston and Myra Cheng, 'Electronic Workplace Surveillance, Part 1: Concerns for Employees and Challenges for Privacy Advocates' (2003) 9 (9) *Privacy Law & Policy Reporter* 161 165.

357 Johnston and Cheng, n 356, 165.

358 Submission 2.

359 See for example, Privacy Committee of New South Wales, n 71, 18.

360 Ibid.

361 Ibid.

employers to replace or update old technology.[362] This issue was raised during consultations, where it was noted that technology providers are to a certain extent driving the use of technology by employers.[363] Johnston and Cheng also state:

> …there has been an unquestioning stampede to harness new technologies in the workplace, such as CCTV surveillance, relational databases and biometric identifiers, to deal with age old problems of performance assessment, employee theft and so on. In many cases, the technologists have been driving both government and private sector policy decisions in the absence of informed public debate. Developments in technology alone must not be allowed to drive our decisions.[364]

3.27 Some employers argue that the problem is not with using surveillance, monitoring and testing practices per se, but arises when managers or supervisors step outside the boundaries of their authority, organisational procedures or culture.[365] An example might be if an IT manager, who is responsible for administering a network, collects and discloses sensitive information obtained from monitoring another employee's email without a valid reason. The Commission believes there is an organisational issue that arises where, as a result of managers overstepping their responsibility, a worker's privacy is disregarded. The organisation should take some responsibility for this, especially if it does not have appropriate policies in place concerning the use of surveillance and monitoring practices.

3.28 At present, employers are not required to consider whether there is a less privacy-intrusive way of managing a situation. Nor are they compelled to implement surveillance and monitoring practices in a way that respects workers' dignity and autonomy. The Commission believes this represents a significant gap in the privacy protection of workers.

---

362 Ibid.

363 For example, Consultations 9, 12.

364 Anna Johnston and Myra Cheng, 'Electronic Workplace Surveillance, Part 2: Responses to Electronic Workplace Surveillance—Resistance and Regulation' (2003) 9 (10) *Privacy Law & Policy Reporter* 187 189.

365 For example, Victoria Police cautions that poor managerial solutions of workplace issues should not be mistaken for privacy-based problems: Submission 31.

### *PHYSICAL AND PSYCHOLOGICAL TESTING AS MANAGEMENT TOOLS*

3.29 Some employers argue they are entitled to utilise various tools to maximise employees' potential.[366] It is also argued that using such tools eliminates bias in assessing performance.[367] This is particularly so in the case of pre-employment recruitment and the use of psychological and selection tests. Some of the advantages employers perceive, include:

- increasing objectivity in assessments;
- being cost-effective;
- adding to the ongoing development of the organisation;
- identifying high achievers;
- increasing productivity; and
- decreasing turnover.[368]

For example, the automotive industry uses pre-employment psychological test results to short-list applicants and provide the basis for future career advice and performance management.[369] However, one commentator makes the point that psychological testing is not a 'cure-all'[370] and cannot be a substitute for good interviewing and management practice.[371]

3.30 Consultations also revealed that psychologists have identified the danger of test use being determined by 'market drive'.[372] An employer representative told us human resources magazines were filled with employer-targeted advertisements for selection and psychological tests.[373]

366 Submission 31.

367 Consultation 2.

368 Peter Saul, 'Psychological Testing in the Selection Process' (1980) 6 (2) *Work and People* 19 19–21.

369 Consultation 13.

370 Adele Ferguson, 'Science, Cynicism and the Cult of Personality Testing', *Business Review Weekly* 23 September 1996 83.

371 Submission 9.

372 R E Hicks, 'Psychological Testing in Australia in the 1990's' (1991) 29 (1) *Asia Pacific Human Resource Management* 94 98.

373 Consultation 13.

## MANAGING LEGAL RISK

3.31 Employers must comply with a variety of legal obligations, ranging from trade practices and consumer protection laws to equal opportunity and occupational health and safety laws. Employers not only have direct legal obligations, but they can in certain circumstances also be liable for the misconduct of workers who breach these laws. Employers told us that for these reasons they use surveillance, monitoring and testing to check up on workers' behaviour. We discuss below some examples of the circumstances in which employers use surveillance, monitoring and testing to help reduce legal risk.

### *USE OF SURVEILLANCE AND MONITORING TO MANAGE RISK*

3.32 Employers told us they use a variety of surveillance and monitoring practices to reduce their exposure to legal liability. For example, businesses might monitor a worker's telephone calls to reduce the possibility of a claim under the *Trade Practices Act 1974* (Cth) for misleading or deceptive conduct.[374] Such claims might occur where, for example, a call centre operator provides a customer with incorrect information about a product or service.

3.33 Employers also justify email and Internet monitoring as a way of detecting and combating worker misuse of the employers' computer systems. An employer may be liable if a worker uses the system to:

- transfer confidential information outside the organisation; [375]
- download or distribute copyright materials;[376]
- post defamatory materials on bulletin boards or via email;[377]
- download pornography;[378]
- distribute inappropriate emails in breach of laws on sexual harassment[379] and bullying; and
- send spam using the employer's email system.[380]

374 *Trade Practices Act 1974* (Cth) s 52.

375 Moira Paterson, 'Monitoring of Employee Emails and other Electronic Communications' (2002) 21 (1) *University of Tasmania Law Review* 1 4.

376 Ibid.

377 Ibid.

378 Ibid.

379 Ibid.

3.34 Managing these issues becomes more complicated where workers use employers' computer technology in places other than the employers' premises, particularly in the workers' own home. Employers are concerned about having less opportunity to directly supervise a worker's computer use in such circumstances.[381]

3.35 Employers also told us they might consider using surveillance to observe workers' behaviour to ensure workers were not bullying each other.[382]

### *PHYSICAL AND PSYCHOLOGICAL TESTING TO MANAGE RISK*

3.36 Under occupational health and safety laws, employers have a duty to provide a safe workplace which includes an obligation to avoid the risk of injury.[383] The duty requires use of preventative measures to minimise injury.[384] Alcohol and drug testing is seen as particularly important where workers are operating dangerous machinery.[385] Similarly, psychological and integrity testing is used by Victoria Police on police officers who carry firearms on patrol and may be required to use varying degrees of force in carrying out their duties.[386] Workers themselves expect the employer to provide them with a safe workplace which would include managing the potentially unsafe behaviour of other workers.[387] This is in addition to the duties employers owe the public generally.[388]

---

380 See *Spam Act 2003* (Cth), particularly s 8.

381 Working from home raises a number of legal issues for employers, such as occupational health and safety issues, potential liability for the conduct of workers and protection of commercial information: see Marilyn Pittard, 'The Dispersing and Transformed Workplace: Labour law and the Effect of Electronic Work' (2003) 16 (1) *Australian Journal of Labour Law* 69 for a discussion of these issues.

382 Consultation 5.

383 Australian Centre for Industrial Research and Training, n 161, 8.

384 Jim Nolan, 'Employee Privacy in the Electronic Workplace Pt 2: Drug Testing, Out of Hours Conduct and References' (2000) 7 (7) *Privacy Law and Policy Reporter* 139 1.

385 Submission 31.

386 Submission 31.

387 Consultation 20.

388 See *Occupational Health and Safety Act 1985* (Vic), s 22 which provides that every employer and every self-employed person shall ensure so far as is practicable that persons (other than the employees of the employer or self-employed person) are not exposed to risks to their health or safety arising from the conduct of the undertaking of the employer or self-employed person.

## USE OF SURVEILLANCE AND MONITORING TO GATHER EVIDENCE

3.37 Surveillance and monitoring is often used by employers to investigate and gather evidence about unlawful conduct or misconduct in the workplace. For example, as we mentioned in paragraphs 3.13–3.15, covert video surveillance is used to gather evidence about theft. The results of email monitoring are produced in cases where workers have been dismissed for misusing an employer's computer system to view or download pornography. It appears that in such cases the Australian Industrial Relations Commission (AIRC) has generally accepted that communications using the employer's computer system may be accessed by an employer and tendered as evidence in proceedings.[389] One commentator has noted that video surveillance usage has increased since the introduction of unfair dismissal laws.[390]

3.38 The justification for using the results of surveillance and monitoring as evidence is that it is likely to be more reliable than human testimony.[391] This might be true generally, but each case should be assessed on its merits. Workers are concerned about being wrongly accused on the basis of video footage. For example, surveillance footage might not be clear[392] or it might not show the whole story. This brings up issues of procedural fairness. A dismissal may be assessed as harsh, unjust or unreasonable if it occurred without consideration to procedural fairness.[393] The philosophy underpinning these provisions is that there should be a 'fair go all round'. We consider that this philosophy should be followed, not only in relation to the use of the results of surveillance and monitoring, but also to the implementation of such practices in the first place.

---

389 Ashley Winnett, *Critically Examine and Assess the Approach of the Australian Industrial Relations Commission to Dismissal of Employees for Breach of Internet and Email Usage Policy* 4.

390 Julian Sempill, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labour Law* 111 127.

391 Ibid.

392 This was mentioned in Consultation 6, though as technology develops this is less likely to be an issue.

393 Section 170CG(3) of the *Workplace Relations Act 1996* (Cth) sets out a number of matters to which the AIRC must have regard in determining whether a dismissal is 'harsh, unjust, or unreasonable'. Several of those matters relate to procedural fairness, namely (i) whether the employee was notified of the reason for termination; (ii) whether the employee was given an opportunity to respond to any reason related to the employee's capacity to perform the role or conduct; and (iii) if the termination related to unsatisfactory performance, whether the employee had been warned about this before the termination (taking into account whether the size of the employer or absence of human resource management expertise in the organisation would impact on any procedures in effecting the termination).

## SECURITY VS PRIVACY

3.39 Since 11 September 2001, security has been an issue for the community at large. The Commonwealth Government has responded to the issue by introducing a number of anti-terrorism measures.[394] The introduction of these measures has fuelled a debate on the extent to which security matters should override our fundamental civil liberties, including the right to privacy. Although perhaps not so dramatic in the workplace context, security is nevertheless an important concern for employers.

3.40 Surveillance and monitoring are used by employers to deal with security concerns in a variety of circumstances. For example, video surveillance can be used to protect workers who work in potentially dangerous or isolated situations.[395] Workplaces such as banks and service stations have video surveillance installed as a deterrent against robberies and to help identify perpetrators. Taxis are now equipped with video cameras which can be activated by the driver if he/she feels threatened.

3.41 In its submission, the Australian Manufacturing Workers' Union discussed video surveillance as a workplace security measure. It agreed video surveillance is generally acceptable for security purposes in sites such as entrances, doors to secluded areas, or areas of restricted access such as contaminated areas and those housing dangerous goods. It may also be acceptable in areas where workers have to work alone or in a particularly dangerous environment. But if surveillance is used in such circumstances, the union argues it should only be implemented subject to a number of requirements. This includes where there is:

- individual consent;
- prescribed purpose for the surveillance;
- potential benefit to the individual concerned;

---

394 For example, the Commonwealth Government amended the *Criminal Code Act 1995* (see schedule 1, part 5.3), to deal with terrorism and introduced the *Suppression of the Financing of Terrorism Act 2002* (Cth), the *Telecommunications Interception Legislation Amendment Act 2002* (Cth) and the *Border Security Legislation Amendment Act 2002* (Cth). State governments have also introduced anti-terrorism legislation. A listing of the relevant legislation dealing with terrorism can be found at <www.aph.gov.au> at 7 June 2004.

395 The safety and security of workers is an occupational health and safety issue for employers. Section 21(1) of the *Occupational Health and Safety Act 1985* states that an employer shall provide and maintain so far as is practicable for employees a working environment that is safe and without risks to health. Section 3 of the Act includes independent contractors as employees for these purposes.

- acknowledgement of collective interests; and
- no jeopardy to collective interests from surveillance.[396]

3.42 Ensuring only authorised individuals enter a workplace (or parts of a workplace) is another security issue for employers. Since 'September 11' there has been a level of anxiety about how to adequately identify individuals. This has led to consideration of biometrics as a means of authenticating an individual's identity. However, as we discussed in paragraphs 2.29–2.30, there are a number of difficulties with biometric technologies and other methods currently appear to be more reliable.

3.43 Over the past few years the security of computer systems has also become a serious issue for many employers. Computer experts reportedly called 2003 'the year of the worm'.[397] If a virus or worm[398] infiltrates an organisation's computer systems it can have serious consequences. Computer hackers and disgruntled workers may threaten the integrity of an organisation's computer systems.[399] The risks posed can range from damage to or alteration of information, theft of trade secrets, fraud and breaches of privacy.[400]

3.44 Employers may resort to computer monitoring to try to prevent or minimise these risks. Good computer security involves a number of integrated measures. For example, computer security should involve measures such as the use of firewalls, up-to-date virus scanning programs and security protocols.[401] It is unlikely that indiscriminate monitoring would be able to effectively safeguard security breaches, but targeted surveillance and monitoring may have a role to play where breaches have been detected.[402] Some random monitoring of computer systems may also assist in assessing potential areas of vulnerability.[403] If such monitoring is used, however, it should be undertaken in a way that minimises privacy invasion.

---

396 Submission 14.

397 see Clive Thompson, 'Dangerous Minds', *Good Weekend: The Age Magazine* 3 April 2003 21.

398 A worm is a program that reproduces itself over a network, usually performing malicious actions, such as using up the computer's resources and possibly shutting the system down: <www.getnetwise.org/glossary> at 5 April 2004.

399 Paterson, n 375, 7.

400 Ibid.

401 Ibid.

402 Ibid 8.

403 Ibid.

## LACK OF CERTAINTY

### *LEGISLATIVE GUIDANCE*

3.45 Some employers told us there is minimal guidance about how to conduct surveillance, monitoring and testing. For example, the Surveillance Devices Act (SDA) says what not to do[404] but does not give an employer guidance on how to implement surveillance measures. One employer group suggested that the surveillance recommendations of the New South Wales Law Reform Commission[405] might be a model for regulation in Victoria as they provide principles and guidance on how to conduct surveillance. [406]

3.46 Another employer said that after randomly drug testing its labour force at one site, every worker tested positive for marijuana use. The question then was what were they to do with the information?[407] Rural employers also shared concerns about what to do with information they might obtain if they conducted drug and alcohol testing.[408]

### *INCONSISTENT STATE AND FEDERAL LAWS*

3.47 A common complaint from employers was that they must balance the requirements of a number of competing regulatory regimes.[409] Not only do employers have to deal with the requirements of occupational health and safety, discrimination and corporations laws, they must also deal with inconsistent state and federal regimes which deal with the same issue. Employers said there are differences between the requirements of federal and state regimes regarding information privacy laws, and surveillance laws vary from state to state. Employers argued that the differences in legal regimes increase business compliance costs. One employer said there is a tendency for business to gravitate towards locations which have the lowest compliance costs. This trend leads to 'lowest common denominator' compliance, which is clearly an undesirable outcome.

---

404 See for example, *Surveillance Devices Act 1999* ss 6(1), 7(1), 8(1).

405 See New South Wales Law Reform Commission, *Surveillance: An Interim Report* 98 (2001).

406 Consultation 5.

407 Consultation 10.

408 Consultation 10.

409 See for example Submissions 11, 26.

3.48 While acknowledging that inconsistencies between federal and state legislation are not ideal, we do not believe this warrants leaving Victorian workers without comparable and comprehensive privacy protection.

### BALANCING OF INTERESTS

3.49 The Commission acknowledges some employers are concerned about workers' privacy and do take it into account in their dealings with workers. The Commission also recognises that employers have a right to manage and control their businesses and to protect themselves against potential legal liability. However, the Commission thinks employers' use of workplace surveillance, monitoring and testing may in some cases be a disproportionate response to the issues they are trying to prevent, limit or manage.

3.50 If an employer has a reasonable suspicion a worker is engaging in misconduct or unlawful conduct, limited and targeted surveillance, monitoring or testing may be justified to confirm or refute that suspicion. However, it may not be justified to use these practices randomly, on the off-chance a worker might be doing something wrong. There may be other less privacy-invasive methods of dealing with management and liability issues, such as educating workers and managers or implementing adequate supervision and performance management systems. Filtering and blocking systems may be more effective than random monitoring in preventing inappropriate email and Internet usage.

3.51 Employers currently get little assistance in determining what is a reasonable use of workplace surveillance, monitoring or testing. As a result, factors other than privacy (such as monetary considerations) are likely to take precedence when an employer makes the decision to implement and use these practices. This is undesirable because it leads to a situation where the interests of employers and the privacy interests of workers are not appropriately balanced.

## WORKER PERSPECTIVES

3.52 During our consultations workers expressed serious concerns about employers' use of workplace surveillance, monitoring and testing. Some of these concerns included:

- the potential for some practices to invade workers' autonomy and dignity;
- lack of transparency about what practices were being used and the reason for their use;
- the effect of privacy invasions on employer/employee trust;

- the practical difficulties which employees have in withholding consent to some practices;
- the inaccuracy of some practices in assessing suitability for work;
- the blurring of the distinction between workers' private lives and working lives; and
- the potential for discrimination as a result of privacy invasions.

## INVADING WORKERS' AUTONOMY AND DIGNITY

3.53 As stated in paragraph 3.6, existing privacy legislation is primarily consumer focused.[410] Accordingly, some commentators argue that a worker's expectation of privacy is largely traded off against the employer's legal control over the worker.[411] They contend that in the workplace, rights to privacy would create 'substantive limitations on the actions and policies of management'.[412] Workers autonomy, wellbeing, dignity, healthy relationships and pluralism within the workplace are pushed aside in favour of, what unions call, 'management exercising control under the guise of its "right" to manage'.[413]

3.54 Although workers may expect a lesser level of privacy at work than in other aspects of their lives, they do not leave their right to privacy at the door.[414] Workers expect to be treated with dignity and respect in the workplace. An obvious example of this is the expectation of a degree of 'private space' in the

410 In terms of consistent workplace privacy protection, information privacy legislation only offers coverage in two areas. The first is the information privacy of Victorian public sector employees (as contained in the *Information Privacy Act 2000*), and the workplace health information of all Victorian workers (as contained in the *Health Records Act 2001*).

411 In Ronald McCallum, *Employer Controls over Private Life* (2000) 20, Professor McCallum expands on this, 'Unless overridden by express contractual terms, all contracts of employment require employees to obey all lawful and reasonable orders, to work with care and diligence, to act with good faith and fidelity, and to maintain mutual trust and confidence between employer and employee'.

412 John Craig, *Privacy and Employment Law* (1999) 76.

413 Peter Holland and Mark Wickham, 'Drug Testing in the Workplace: Unravelling the Issues' (2002) 18 (1) *Journal of Occupational Health and Safety Australia and New Zealand* 55 58.

414 See for example, Submission 25 in which the Victorian Bar states that privacy is inherently limited in the employment context because the employee is acting as the employer's agent, and in carrying out the tasks of a particular job may well be acting in the full public gaze. However, this does not mean the employee's private life ceases to be a matter worthy of protection. The Bar states that the right to privacy should only be restricted when a clear case has been made that there is a more pressing or predominant social objective, such as the need to protect public health and safety, the legitimate business interests of the employer or the legitimate interests of third parties.

workplace, such as in toilets, change rooms, locker areas and lunch rooms.[415] Employers appear to grapple with a proportionate response to these expectations. For example, during our consultations some employers said that while they might consider installing surveillance cameras in areas such as canteens as a deterrent to bullying and other such behaviour, they would be reluctant to record conversations as part of that surveillance.[416] This was thought to be too intrusive in areas where workers have the right to have private conversations during breaks.[417] The law seems to provide little external guidance in determining how such issues are to be resolved.

## LACKING TRANSPARENCY OVER PRACTICES BEING USED AND THE REASON

3.55 During our consultations, unions expressed concern that employers do not adequately communicate workplace surveillance, monitoring and testing policies to workers.[418] This concern appears to be backed up by the unions' experience of inconsistencies among employers as to whether they have workplace surveillance, monitoring and testing policies. If policies exist, the manner and extent to which they are communicated to workers seems to vary.[419]

3.56 Unions cited instances where workers were told surveillance or monitoring would be used for one purpose, but in practice was used for a different purpose.[420] An employer might legitimately place a surveillance camera in a car park for security, but then use the information collected from the surveillance to determine whether a worker's compensation claim is genuine.[421] We were informed that surveillance cameras or monitoring systems were often established in the workplace without any advance notice or consultation with workers.[422]

---

415 Privacy Committee of New South Wales, n 71, 41. There is a prohibition on employer surveillance of employees in any change room, toilet, bathroom or shower facility, contained in s 9(3)(b) of the *Workplace Video Surveillance Act 1998* (NSW). See also cl 9 of the Exposure Draft of the Workplace Surveillance Bill 2004 (NSW).

416 Consultation 5.

417 Consultation 5.

418 For example, Consultations 8, 11 and 12.

419 Ibid.

420 Consultations 8, 11, 12.

421 Consultation 12.

422 Consultation 12.

## EFFECT OF PRIVACY INVASION ON EMPLOYER/EMPLOYEE TRUST

3.57 Apart from privacy considerations, some commentators note these practices also seem to contravene the employer's implied duty of trust and confidence in the worker.[423] As one submission argues 'an employee's right to privacy is violated whenever personal information is requested, collected or used by an employer in a way or for a purpose that is irrelevant to or in violation of the contractual relationship that exists between employees and employer'.[424]

3.58 One commentator suggests other practices may undercut the employer's duty of trust and confidence. For instance, the introduction of random testing by the employer of all workers stems from a presumption of the workers' guilt—a presumption that workers are required to rebut regardless of work performance.[425] Some commentators advocate the duty of trust and confidence as having the potential to place limits on the discretion of the employer within the work relationship, such as with the misuse of policies.[426] However, the potential use of the duty in this manner is limited in certain important ways.

3.59 The duty is only implied within an 'employment' relationship and may not extend to other types of workers.[427] There is also uncertainty about whether an expressly agreed term in a contract can limit the scope of this implied duty[428] which, in the individual bargaining context, would easily be dominated by the employer's requirements. As with these types of claims, the uncertainty and inappropriate remedies, coupled with the costs and time involved in going to court,[429] makes enforcement of the duty on a stand-alone basis unlikely.

---

423 Lord Steyn in *Malik v Bank of Credit & Commerce International SA (In liq*) [1998] AC 20 at 53 determined that 'the implied mutual obligation of trust and confidence applies only where there is "no reasonable and proper cause" for the employer's conduct, and then only if the conduct is calculated to destroy or seriously damage the relationship of trust and confidence'.

424 Submission 16.

425 Caroline Morris, 'Drugs, the Law, and Technology: Posing Some Problems in the Workplace' (2002) 20 *New Zealand Universities Law Review* 1 38.One union recalled an instance where a number of long-serving workers viewed the sudden introduction of general alcohol and drug testing as a breach of trust by their employers given their long-standing service to the company: Consultation 19. See also Submission 1.

426 Kelly Godfrey, 'Contracts of Employment: Renaissance of the Implied Term of Trust and Confidence' (2003) 77 *Australian Law Journal* 764 770.

427 Ibid 771.

428 Ibid 771, and see Sempill, n 390, 129.

429 Sempill, n 390, 131.

Consequently, the protection the duty affords in relation to privacy concerns seems minimal.

## PRACTICAL DIFFICULTIES OF EMPLOYEES WITHHOLDING CONSENT

3.60 A central concept in labour law is that of a worker's 'consent'. This means 'a voluntary agreement, the act or result of coming into accord. It is an act that is unclouded by fraud or duress'.[430] However, a number of commentators point out that 'the employer/employee relationship is marked by such a power imbalance as to vitiate any notion of free consent'.[431] Accordingly, within the standard work relationship, consent becomes increasingly difficult to refuse,[432] particularly where the perceived consequence of refusal is to place the employee under considerable duress. As such, 'employees who want to keep their jobs or apply for one in the first place, may effectively be forced into compromising their own privacy'.[433] One commentator puts it this way:

> Can there be any doubt that the employer exercises power of life and death over each of us at least as great as the power of government? The power to deprive us of our livelihood, often with no notice…the power to lay off, to transfer to an undesirable community, to reassign to an unhappy job. The power to make us miserable. The power to strip us of our identity, to the extent that our vocation is our identity.[434]

3.61 In the context of testing, the UK Draft Code of Practice tries to address this issue by deeming that 'consent will not be freely given if the penalty for not consenting is dismissal'.[435] The code goes on to state that even where there is valid consent, the processing of personal data may be found to be unfair 'if taking into account the circumstances in which consent is obtained, the employer uses its dominant position to carry out testing even though the benefits do not outweigh the inevitable intrusion into privacy'.[436]

---

430 Information and Privacy Commissioner, *Workplace Privacy: A Consultation Paper* (1992) 22.

431 Morris, n 425, 27.

432 Submission 1.

433 Morris, n 425, 29.

434 Information and Privacy Commissioner, n 430, 22.

435 Submission 1 and Office of the Data Protection Commissioner, *The Use of Personal Data in Employer/Employee Relationships* Draft Code of Practice (2000) 35.

436 Ibid.

3.62 Quite apart from the issue of discrepancy in power between the employer and worker, unions argue the 'consent' approach also assumes workers understand the implications of the practices to which they are agreeing.[437] The concept of consent requires full knowledge of the matter, yet some workers can underestimate the consequences. Unions cited instances where, in consenting to a psychological test, a worker's 'striking sense of shame if they performed less effectively than expected'[438] and the consequences that had on their self-esteem could be devastating. One union drew a parallel with this and the aftermath of testing positive to the presence of drugs and/or alcohol.[439] When workers overuse prescription drugs or have a couple of drinks during lunch, the assumption can be that they are drug addicted or an alcoholic—in the workplace, where mud can and does stick, this can lead to workers' victimisation.[440]

3.63 A number of unions said psychological, behavioural and integrity tests were endemic in the pre-employment context and were frequently used by recruitment agencies as prerequisites for workers getting jobs.[441] We were informed that consent to various forms of testing tended to be verbal, or was sometimes just assumed.[442] An employer representative noted there was generally no resistance to pre-employment testing.[443]

3.64 We were advised that the consent sought for psychological testing tended to be broad rather than specific in nature,[444] putting further into doubt the worker's 'knowledge' of the consequences of testing (as already discussed). Another example of this is when an employee consents to a medical report being disclosed to the employer, where little prevents a doctor disclosing to the employer more than is strictly required for the position.[445] This is particularly pertinent since the protections offered by the implied duty of trust and confidence and the implied duty to obey lawful and reasonable orders can be overridden where the

437 Submission 2.
438 Ibid.
439 Consultation 19.
440 Ibid.
441 Consultation 11.
442 Consultation 9.
443 Consultation 10.
444 Consultation 2.
445 Consultation 9.

employee consents to such practices.[446] One union noted that in the transport industry, alcohol and drug testing was increasingly being contracted out to agencies in circumstances where applicants tended to be young people applying for their first jobs.[447] Applicants were typically informed that the consent they had provided entitled the job agency to retest them every six months.[448]

3.65 This issue is also identified in the UK Draft Code of Practice, where it acknowledges that consent is virtually meaningless in the pre-employment context. The Code therefore recommends voluntary alcohol and drug testing only be undertaken after an offer of employment.[449] This view is similarly supported by the Privacy Committee of New South Wales in its Drug Testing in the Workplace Report.[450]

3.66 Consent is also an issue in the context of workplace surveillance. Although the SDA provides some protection against surveillance, there are significant limitations to its application. In particular, the SDA does not apply to the use of a device where the person subject to surveillance has agreed to it.[451] Workers may have little practical capacity to object to surveillance in the workplace for the reasons stated above.

3.67 The SDA states consent can be either express or implied[452] but there is no indication of what constitutes implied consent. For example, would the introduction of a policy which says the employer can use surveillance amount to implied consent?

3.68 The trend of placing surveillance, monitoring and testing requirements in company policies usually means workers 'agree' in their contracts to employers

446 See Bliss n 156.

447 Consultation 11.

448 Consultation 11.

449 Submission 1.

450 'Unless a refusal to take a drug test truly has no consequences for the employee or job applicant then any consent obtained prior to the test cannot be considered to be freely given. Workplace drug testing is rarely voluntary and refusal to submit to a test usually results in counselling or disciplinary action such as transfer, demotion or dismissal. In the case of pre-employment testing, it can be more easily argued that job applicants have freely consented to drug tests, as they can simply withdraw their applications if they object to testing. But missing out on a job opportunity is as much a penalty for refusing to undergo a test as demotion or dismissal': Privacy Committee of New South Wales, *Drug Testing in the Workplace* No 64 (1992) 12.

451 See *Surveillance Devices Act 1999* ss 6(1), 7(1) and 8(1).

452 See *Surveillance Devices Act 1999* ss 6(1), 7(1) and 8(1).

unilaterally altering policies 'as advised from time to time'. This simply requires notification of such practices or policies and does not require the specific consent of the worker to such changes. While the requirement of consent (a requirement unions have long preferred) is perhaps more 'consultative' and less paternalistic than a mere notification of a change in employment terms and conditions, 'consent' as a concept is perhaps a fiction either way. As one commentator explained it, in the context of privacy, the assumption seems to be if you object you resign, which has the effect that workers are only provided with as much privacy as the employer is willing to tolerate.[453]

## BLURRING THE DISTINCTION BETWEEN PRIVATE AND WORKING LIFE

3.69 The relationship between worker and employer can extend beyond the boundaries of the traditional workplace. This is most evident in relation to testing practices.

### *TREND TOWARDS 'SELF-TESTING'*

3.70 Testing raises important questions about what should be permitted within the work relationship as against a worker's right to autonomy and dignity. For instance, union consultations suggest there is an employer trend towards 'do-it-yourself' take-home test kits[454] and self-education. The 'take home' approach requires workers to use their private time to undertake tests for a work-related purpose.

3.71 Unions argue this is part of a philosophical shift away from employers taking responsibility for worker safety, making it instead the workers' responsibility.[455] They see it as exposing a gap in the protection of laws—namely the extent to which employers can impinge upon workers' autonomy outside work hours.[456] In doing so, workers are 'expected' though not 'directed' to violate their own bodily privacy for a work purpose.

453 Craig, n 412, 82.

454 The practice of 'take home test kits' was raised in Consultation 4 where certain employers make available to workers take home do-it-yourself kits, which encourages workers to take responsibility for testing themselves at home to give them some indication of their alcohol and/or drug levels.

455 Consultation 4.

456 Consultation 4.

### *TESTING CAN REVEAL PRIVATE INFORMATION*

3.72 The testing process itself can also lead to disclosure of private medical information. Workers may be required to disclose their full personal medical histories during a test. Although this disclosure may be to a doctor in the context of medical testing, there is some debate[457] as to whether a traditional doctor–patient relationship exists in these circumstances.[458] Either way, the information can be disclosed to the employer if the worker consents to it (the problems arising here with respect to consent have already been discussed).[459]

### *THE POTENTIAL FOR DISCRIMINATION AS A RESULT OF PRIVACY INVASION*

3.73 Union consultations revealed a similar situation with alcohol and drug testing, where workers are usually required to provide a list of all medication *directly* to the employer to exclude it from any drug and alcohol test results.[460] In providing this information, medical conditions irrelevant to the performance of work may be communicated to the employer. Depending on the condition, this may even lead to indirect disclosures about the medical conditions of the worker's family members. Information of this kind can lead to a risk of unlawful discrimination. For example, it may be assumed someone is disabled in some way (eg a psychological condition), is of a particular sexual persuasion,[461] or is trying to get pregnant—all of which are attributes protected under anti-discrimination legislation.[462] Of particular relevance with drug and alcohol testing is the possibility that an 'addiction' could also be determined to be a 'disability' in certain anti-discrimination jurisdictions.[463] But apart from reactive anti-

457 See paras 2.42–2.45.

458 Ibid.

459 Ibid and paras 3.60–3.68.

460 Submission 1, Consultation 18.

461 Based on stereotypical assumptions, it is possible that sexual persuasion can be imputed from, for instance, the presence of HIV-related drugs.

462 See for example *Equal Opportunity Act 1995* n 158 and n 308.

463 See Submission 1. See in particular the case of *Marsden v HREOC 7 Coffs Harbour & District Ex-Servicemen & Women's Memorial Club Ltd* [2000] FCA 1619 (15 November 2000) where the court found that a drug addiction was a protected disability. The NSW Government responded to this decision by introducing legislation preventing employees from claiming drug-addiction of a prohibited drug as a disability (see *Anti-Discrimination Act 1977* (NSW) s 49PA 'Persons Addicted to Prohibited Drugs').

discrimination laws and privacy collection principles,[464] little exists to prevent this kind of communication occurring in the first place.

3.74 Additionally, some unions said requiring workers to reveal complete medical histories to employers limit their ability to be autonomous, as well as undermine the concept of dignity by treating workers as 'things' to test for 'current chemical composition'.[465] This gives rise to questions of balance—is such an invasive disclosure proportionate to the benefit of detecting the presence of drugs or alcohol, which may have little or nothing to do with their capacity to do their jobs? Are there other ways to manage this risk that do not involve this kind of disclosure, such as performance management through goal setting or counselling? Can such an invasive disclosure ever be justified in the context of random (no cause) testing?

### *After Hours Lifestyle and The Inaccuracy of Some Practices in Assessing Suitability for Work*

3.75 Another concern arising from union consultations was the increasing encroachment of employers on workers' after-hours lifestyles. One commentator observed 'a shift in the nature of the employment relationship…has led to limited circumstances where out of hours conduct may result in adverse consequences for a person's employment'.[466] One example of this is tests that identify the presence of drugs and alcohol that may reveal substances which have been consumed outside of work hours. The 'chemical window' of certain testing processes can extend back months, and could include a period prior to the worker even being employed.[467] It would be difficult to sustain an argument that this kind of testing window could ever be a proportionate response to ascertaining a worker's current state of drug and/or alcohol impairment.

3.76 The technologies involved in testing for drugs and alcohol can reveal information about people's lifestyles that falls well beyond the control an employer would otherwise be expected to exert in a 'work relationship'. From cases involving after-hours conduct, a test has been developed that objectively requires the employee's conduct to be likely to cause serious damage to the

464 These principles govern the way the employer collects the information (see for example *Health Records Act 2001* Health Privacy Principle 1).

465 Consultation 4 and Submission 9.

466 Nolan, n 384, 6 and *Rose v Telstra* (unreported AIRC), 4 December 1998, Print Q9292 at 7–9.

467 See paras 2.72–2.92 for a detailed discussion of alcohol and drug testing.

relationship of employee and employer, or is conduct that damages the employer's interests or is incompatible with the duty of the employee.[468] This involves assessing the facts of each case. At the same time, a continuing tension exists between the employer being entitled 'to establish work conditions which workers knowingly submit to' (often reflecting various other statutory duties employers owe)[469] and the employer not having the disproportionate or 'unfettered right to sit in judgment of out of work behaviour'.[470]

3.77 One union submission stated that what workers do in the 24 hours before their scheduled start to work is their business, as this is private time out of the workplace.[471] Workers have a right to a private, autonomous life away from work. For example, in one case it was held that a dismissal for drug use was a prohibition on lifestyle.[472]

3.78 On the other hand, employer groups are being advised their responsibilities within the work relationship are not necessarily confined to the terms of the contract, and some incursion into workers' private lives may be warranted if there are implications for the employer and the workplace. According to one employer submission, the question is not about interference with privacy, but whether such interference is warranted in the circumstances.[473]

3.79 This is compounded by the fact that the work relationship is taken to include, in certain circumstances, pre- and post-employment obligations. This broadening of employer responsibilities, arising by virtue of a proposed or former work relationship, provides a strong argument for an employer to adopt an 'expansive' rather than a narrow view of the relationship. For instance, in the pre-

468 Nolan, n 384, 5. See *Rose v Telstra* (unreported AIRC), 4 December 1998, Print Q9292 which at 6–7 further states that 'in essence the conduct complained of must be of such gravity or importance as to indicate a rejection or repudiation of the employment contract by the employee…absent such considerations an employer has no right to control or regulate an employee's out of hours conduct'.

469 Craig, n 412, 74.

470 Nolan, n 384, 7. See also *Rose v Telstra* (unreported AIRC, Vice-President Ross, 4 December 1998, Print Q9292) at 14.

471 Submission 9.

472 Robbie Walker and Ballanda Sack, 'Drug and Alcohol Testing' (2003) (12) *OHS Alert* 1 3—'the Commission found that while it was common sense to dismiss a train driver for drug use or possession on duty, dismissing him for using the drug (marijuana) was a prohibition on lifestyle rather than workplace conduct'. The employee had informed the employer he had ingested the marijuana after hours on a Saturday at a party: *James Charles Debono v Transadelaide* 1031/99 S Print R8699, 7 September 1999, AIRC per Raffaelli C.

473 Submission 29.

employment context, job applicants are also protected by occupational health and safety, discrimination, information privacy and trade practices laws. The employer is potentially liable for breach of legal obligations in all these areas. In the post-employment context, employers can still owe former workers entitlements, such as the duty to provide a fair and accurate reference, payment of outstanding wages and remittance of outstanding superannuation contributions. Interestingly, some medical testing consultants even offer post-employment medical testing services.[474] The adoption by employers of an expansive view of the work relationship is likely to impact on when and how they use practices to manage these obligations.

3.80 This approach is reflected in cases which have determined that in certain situations, employer responsibility (and liability) is not just limited to work activities, but can encompass off-duty activities.[475] There will be situations where medical examinations in workplace settings are necessary to the interests of public health and safety or to determine eligibility for benefits under the WorkCover scheme.[476] Some employer groups argue that alcohol and drug testing is based on the community expectation that employees in certain occupations will not be adversely affected by substances.[477] This seems particularly so with respect to safety sensitive positions.

### *BLURRING OF MANAGEMENT WITH SOCIAL CONTROL?*

3.81 In the absence of similar cases or express legislative requirements, the issue of what falls within the scope of the work relationship is usually left to the employer (as the more powerful party) to determine. In accordance with the test outlined earlier, the employer would need to decide, first, when activities in a worker's private life seriously impact on the work relationship and secondly, whether these activities come within the responsibilities owed (broadly or otherwise) by the worker as part of the work relationship.

---

474 One test provider states 'Post-employment medicals are recommended to establish an exiting employee's medical status. This process is particularly useful in matters such as Workers' Compensation and Occupational Health and Safety issues. They are particularly useful when employees may have had exposure to chemicals or any other occupational hazard', see *'Pre and Post Employment Medicals'* (2003) Corporate Medical Options .

475 Nolan, n 384, 1.

476 Submission 29. See also s 112 of the *Accident Compensation Act 1985* which requires workers to submit to a medical examination.

477 Submission 31.

3.82 Yet, our union consultations indicate this type of evaluation does not always occur. For instance, with drug and alcohol testing, one of the principal objections by various union groups is that such processes do not test for actual 'impairment' of workers by drugs and/or alcohol, but rather for their 'presence'.[478] A submission highlights this point:

> To say that employers can use drug testing to prevent harm is not to say that every employer has the right to know about the drug use of every employee.[479]

3.83 It is arguable that impairment in work functions caused by drug and alcohol abuse (whether at or outside work) may fall within the scope of the work relationship. However, it is far less likely that the mere presence of alcohol and/or drugs in a worker would be similarly covered

3.84 The line between effective management and forms of social control therefore becomes increasingly blurred. Given the unequal bargaining power of the parties, the 'innocent have nothing to fear' rationale provides little restraint on the actions of the employer.[480] This has led to union concerns that employers are acting as 'de facto police'[481] and that 'the State should not be permitted to recruit employers'[482] to monitor a worker's (read private individual's) drug and alcohol consumption. If it is accepted that the identity of the private individual is not simply that of a 'worker', it is then questionable that under existing surveillance legislation the individual as a private citizen is given more protection than the same individual as a worker.

### *PHILOSOPHICAL OBJECTIONS TO EMPLOYERS COLLECTING CERTAIN INFORMATION*

3.85 Some workers simply have an outright philosophical objection to the collection of certain information by their employer. This attitude was most clearly apparent in relation to the use of biometric technologies.[483] Fingerprints and finger scans are usually associated with criminal behaviour and they have that connotation for some workers, even when taken by their employer. Workers are

478 Consultations 11, 19 and 21.

479 Submission 16.

480 See Holland & Wickham, above n 368. See also Submission 16 for further discussion.

481 Kathryn Heiler, 'Drugs and Alcohol Management and Testing Standards in Australian Workplaces: Avoiding that "Morning-After" Feeling' (Paper presented at the Drugs and Alcohol at the Workplace: Testing Issues and After Hours Conduct: Breakfast Briefing, Thursday 5 December 2002, Sydney) 3.

482 Craig, n 412, 189.

483 Consultation 12.

concerned biometric systems may enable their employers to collect unnecessary information. For example, retinal scans have the potential to reveal information about an individual's health.[484]

## TESTING AND THE 'FIT' WORKER

3.86 Employers are increasingly using testing to determine whether workers will 'fit' into the work environment, either physically or psychologically.

### *FITNESS FOR WORK*

3.87 A number of unions are concerned about the shift in the onus of primary responsibility from the employer to the employee on issues like safety, and the impact this can have on workers' privacy. This ties in with the notion of an employee's 'fitness for work'. This concept commonly appears within Australian contracts of employment and collective agreements as an express term requiring an employee to be 'fit for work'. The term seems capable of extending beyond any implied duty of 'obedience and cooperation' (which is limited to what is considered reasonable in the circumstances), or the duty of due care and skill (the breach of which case law has interpreted to require a serious breach).[485] 'Fitness for work' seems to surface predominantly in the occupational health and safety (OHS) context, though unions claim it is a different concept to OHS.[486] In the context of testing, unions argue that fitness becomes an issue of control, and is less about health and more about discipline[487]—with workers privacy the first casualty.

3.88 An example of this is the issue of fatigue. Under fitness for work requirements, a tired employee may be at a higher risk of making a mistake, of producing lower quality work, or creating a dangerous safety hazard. Arguably then, a fatigued employee could be classified as unfit for work. Does this then mean an employer could compromise a worker's autonomy by directing them to change their lifestyle, such as imposing a bedtime curfew? Would workers have a

484 The state of the retina changes with various clinical conditions such as diabetes, glaucoma, high blood pressure and ageing. An employer could conceivably gain an insight into the state of a worker's health by taking daily retinal scans. However, there is reportedly no medical evidence that the iris, which is also used in biometric systems, has any correlation with a person's health: Lane, n 79, 72–3.

485 For detail on these concepts see Creighton and Stewart, n 18, 248–51.

486 Consultation 21—Unions suggest the concept of 'fitness for work' includes issues of good and bad performance and discipline which stray beyond what is contemplated by occupational health and safety issues.

487 Ibid.

responsibility to turn up to work 'well-rested, alert and dynamic'? The worker may be fatigued because of longer work hours or weekend work, or a personal reason they do not wish to disclose. Some unions believe employers should be looking at OHS as a holistic 'system'[488] rather than an individual fitness problem left to the worker to identify and rectify—preferably in their own time. A gap in protection exists where an employer can include a 'fitness to work' requirement in a worker's contract and subjectively define it thereafter (and unilaterally incorporate the privacy-invasive practices used to measure it).

3.89 Undertaking genetic testing[489] as part of a 'fitness to work' examination may be particularly harmful as results could identify diseases for which there is no current treatment or cure.[490] During our consultations, a number of unions said one of the strongest incentives for employers to use testing was to identify pre-existing injuries to obtain a pre-emptive release of liability under the *Accident Compensation Act 1985*.[491] Unions see this as contrary to the philosophical principle that an employer must 'spread the risk in taking the worker as you find them'.[492]

3.90 From an employer's perspective, workers have their own specific obligations under the *Occupational Health and Safety Act 1985*. Accordingly, if the unions' 'holistic' approach is adopted, it must necessarily include the individual responsibilities workers themselves have in maintaining a safe workplace. Employers can feel as though they are placed between 'the devil and the deep blue sea'[493] when legal obligations 'often give the appearance of imposing apparently contradictory demands'.[494] OHS legislation imposes an onerous duty on employers to avoid the risk of injury.[495] The legislation is not overly prescriptive,[496]

488 Ibid—it was suggested by unions that testing focuses on the behaviour of workers rather than employers' work systems.

489 Submission 1. In Submission 29 the Office of the Victorian Privacy Commissioner submits that 'Genetic testing may be considered to offend fundamental rights and freedoms, not only because it may be imposed but because it denies an individual the "right not to know" or to have others know…results of tests may be particularly harmful in circumstances where results identify diseases for which there is no current treatment or cure. Test results may also be used to deny work opportunities (possibly in breach of equal opportunity and/or disability discrimination laws)'.

490 Submission 29.

491 Consultation 11.

492 Consultations 4 and 21.

493 Australian Centre for Industrial Research and Training, n 161, 5.

494 Ibid.

495 Ibid 6–8. See also s 21 of the *Occupational Health and Safety Act 1985* (Vic).

which is perhaps a recognition of the diversity of workplaces and the need for flexibility in application. But this flexibility creates uncertainty concerning the scope of employers' obligations under the OHS regulatory scheme.[497] Given this, it is not surprising most law on 'fitness to work' varies according to the facts of the specific case, and leaves employers with the unenviable task of striking a 'careful balance between their legal obligations and concern for their employees' rights and dignity'.[498] When employers have been overzealous in their approach, and have failed to take action proportional to the risk, industrial tribunals have found against them.[499]

3.91 But where is the line to be drawn when evaluating the safety of another worker or a member of the public? When can privacy concerns outweigh the elimination of a risk, however small, if it prevents a death or injury? The gravity of the issue is not lost on the union movement which has made its own concession to the inclusion of alcohol and drug testing regimes within numerous industrial agreements.[500] Many unions concede that alcohol and drug testing may be needed in hazardous or safety sensitive positions, particularly where adequate supervision may not be possible.[501] As stated in one union submission:

> It seems logical to allow mandatory drug and alcohol testing only where safety is an inherent requirement of the occupation…[creating a] consistent workable balance between occupational health and safety, privacy and equal opportunity legislation.[502]

3.92 The Victorian Trades Hall Council suggested testing must be 'fair in all the circumstances' and must not be excessive or unreasonably intrusive.[503] Still a number of unions asserted that alcohol and drug problems were not workplace specific but a community problem that should be addressed with educational programs, counselling and honour systems.[504]

---

496 Ibid 9.

497 Ibid 9.

498 Ibid 10.

499 Ibid 24–5.

500 Ibid 29.

501 Craig, n 412, 197. See also Consultations 4 and 19.

502 Submission 1.

503 Submission 1.

504 Consultation 11.

3.93 However, the question remains, is testing for fitness justified for all 'imaginable kinds of exclusionary criteria simply because the scientific means to do so exists'?[505] Put another way:

> we must ask whether it is right that employers should be allowed powers in the workplace to police their employees' conduct, simply because there is technology that makes it possible.[506]

3.94 The employer's task is made more difficult when all they have to base their decisions on is fact-specific case law and their subjective understanding of a reasonable common sense approach[507] to concepts of privacy.

### *CULTURAL FIT*

3.95 'Fitness for work' can include 'mental' as well as 'physical' fitness. For instance, some unions believe psychological testing could create a class of unemployable people.[508] A revealed 'predisposition to stress', for example, would not necessarily mean the person is incapable of performing the job and performing it well.[509] The Victorian Privacy Commissioner raised a number of objections to the use of psychological tests in the workplace:

> Psychological test results are open to very wide interpretation by both employees and workers. Many tests may not be culturally sensitive for particular workers …
> Psychological testing may have inherent validity and reliability issues, coupled with the fact that test results may stigmatise or label a subject.[510]

3.96 As discussed in Chapter 2 (see paras 2.68–2.71), there is inconsistent regulation of the various types of psychological tests. Furthermore, there is little regulation of how the employer eventually decides to use the test results and whether privacy is a consideration.[511] Where decision-making is at the employer's discretion, it can be very difficult to prove claims such as discrimination because other 'objective' factors such as attitude or team skills, could be used to mask this (see paragraph 2.71 for discussion of potential issues surrounding psychological

505 Australian Centre for Industrial Research and Training, n 161, 38.

506 Morris, n 425, 25.

507 Ibid 37–8.

508 See for example Consultation 4.

509 Consultation 21.

510 Submission 29.

511 See Psychological Testing paras 2.68–2.71.

testing and discrimination). One commentator raised the example of tests that included unnecessary questions on religion and sexuality as a part of a rationale not to employ unstable people.[512]

3.97 Some consultation groups commented on the term reasonable or cultural 'fit' in relation to psychological tests,[513] particularly as more employers are using psychological testing processes to select job applicants who have the necessary 'cultural fit' with the team and/or organisation.[514] One submission states:

> Management tends to prefer employees who follow rather than challenge established practices where servile employees are perceived as less threatening, even though these individuals tend to stifle progress and development.[515]

3.98 According to this view, employers are more likely to underestimate the skills and qualities of employees whose values do not align to the general 'moral principles' of the organisation.[516] Although psychological tests are usually marketed as providing an objective hiring basis, notions of cultural fit can mean bringing privacy invasion and discrimination in through the back door. Measures of cultural fit can involve seeking information about the worker that extends beyond what the job requires, intruding into the realm of private information. Detailed questions about social habits, likes and dislikes or views on authority[517] can help paint the desired picture of 'cultural fit'.[518]

---

512 Craig, n 412, 79–80. It should be noted that while state and federal discrimination laws protects certain attributes from being used as the basis for discrimination, it will not extend to cover all types of personal information. Even where discriminatory questions are being asked in the pre-employment context, for similar reasons as that discussed above, fear of not getting the job, or being black-listed from the industry, means very few cases of this kind are brought in the discrimination law jurisdiction—see Submission 22 for a more detailed discussion of the context to these problems.

513 Consultation 2 and Consultation 11.

514 Statistics on usage by employers of psychological tests are referred to in Chapter 2, para 2.51.

515 Submission 2.

516 Ibid.

517 Questions eliciting this kind of information may not be covered by a protected attribute under anti-discrimination legislation (see for example s 6 of the *Equal Opportunity Act 1995* (Vic) which has one of the most extensive list of protected attributes within the Australian anti-discrimination jurisdiction, and which would not capture most of the above-stated information).

518 Consultation 4—here a representative of a union stated that psychological tests only tested 'patches of behaviour' which does not constitute the 'personality'. Although conceding skills tests may be appropriate, tests that inferred an inherent or long-term personality trait were seen as unacceptable.

3.99 Another union argument is that concepts of 'fitness for work' and/or 'cultural fit' can be used by employers to target certain individuals[519] or perceived troublemakers (eg a union member or a worker who makes a sexual harassment complaint) who 'don't fit'. Selection tests can also be geared to identify individuals who will conform strictly to lines of authority. Workers who, in certain circumstances, may criticise management decisions or choose to enforce their rights through grievance mechanisms, may still be entirely capable of performing the inherent requirements of their position. These kinds of qualities are private and personal to individuals, and central to workers' autonomy in asserting their rights and protecting their dignity.

3.100 One union argued that the notion of worker impairment (whether mental or physical) is increasingly 'self-referential', becoming more concerned with a person's human capacities than the inherent requirements of the position.[520] This is compounded by an absence of a guarantee that the worker will be tested against core, as opposed to non-core, position requirements.[521] As stated in one submission, 'employers do not have an inherent right to medical information. Potential employees, instead of being accepted on their individual merits and academic achievements, are being put through a selection process based on their blood results'.[522] The same could be said of psychological test results.

3.101 The combining of 'physical' and 'mental' fit can be seen most clearly in the context of alcohol and drug testing. Unions indicated that in certain industries where alcohol and drug testing have become routine, zero blood alcohol test results have come to mean 'fit for work'.[523] A number of commentators argue that while the focus remains on employers seeking often scant evidence of potential drug abuse,[524] drug and alcohol testing is at the same time being used to relieve the employer from making performance-based decisions altogether.[525] Setting aside the obvious physical fitness issues, mental 'fitness' or 'fit' can arise where test results are interpreted in accordance with moralistic stereotypes,[526] that is 'no

519 Consultation 19.

520 Consultation 4.

521 Ibid.

522 Submission 4.

523 Consultation 11.

524 Morris, n 425, 34.

525 Craig, n 412, 193.

526 Ibid. See also Ferguson, n 370 for a critique of the use of stereotypes in psychological testing.

alcohol and drugs/good worker' versus 'alcohol and drugs positive/bad worker'.[527] Where this occurs, such testing can take the form of a back-door integrity test. This allows the employer to shift the onus entirely on to the worker to 'fit' and be 'fit'.

## THIRD PARTIES

3.102 By third parties we generally mean people who are not workers or employers. These can include customers, suppliers, family and friends. The interests of third parties in relation to workplace privacy can arise in a number of circumstances. Third parties can be involved in the processes of surveillance, monitoring and testing, and the obligations and/or interests of these parties may come into conflict with the privacy interests of workers. These issues are discussed below.

### SURVEILLANCE, MONITORING AND TESTING INVOLVING THIRD PARTIES

3.103 Sometimes employers use third parties to conduct surveillance and monitoring. One example of this might be where employers use private investigators to find out whether a worker is on genuine sick leave. Another is the use of 'mystery shoppers', who may be hired by the employer to assess the performance of customer service staff.[528] Apart from the provisions of the Surveillance Devices Act[529] and information privacy legislation[530] (in relation to the collection of information about an individual) there is no other regulation of the use of covert surveillance in this manner. The Federal Privacy Commissioner has issued *Covert Optical Surveillance in Commonwealth Administration: Guidelines* for Commonwealth agencies conducting covert optical surveillance of people claiming compensation. Although not intended for the private sector, the Guidelines could be followed by private sector employers as 'best practice'.

3.104 Another example is where an employer uses a third party to monitor emails or observe video monitors. If the third party records personal information about workers, the provisions of the Privacy Act will apply to the collection and

527 Craig, n 412, 193.

528 See Chapter 2, para 2.35.

529 See Chapter 2, paras 2.16–2.17 for a discussion of the *Surveillance Devices Act 1999*.

530 See Chapter 1, paras 1.20–1.24 for a discussion of information privacy laws.

handling of that information.[531] However, as is the case when the practice is conducted by the employer, there is limited privacy protection for workers in relation to the practice itself. An employer could seek to safeguard workers' privacy by setting out privacy obligations in its contract with the third party service provider. However, we were told during consultations it is not common for employers to have such arrangements in place.[532]

3.105 Third parties are often used to store alcohol and drug test results.[533] Our consultations also revealed a trend by employers to engage recruiters to select, conduct and store psychological test results.[534] The use of company or company-selected doctors and nurses may also constitute third parties, as would behavioural health counsellors, health and safety representatives, rehabilitation providers and counsellors engaged through employee assistance programs—all of whom have access to workers' private information. Although, as previously discussed, the provisions of the Health Records Act apply to 'health information'[535] it is unclear whether this term includes all alcohol and drug and psychological-type test results.

3.106 The privacy of third parties can also be impinged upon in the workplace. One example is where a visitor to a workplace is captured on surveillance footage. Another is where the contents of an email from a third party are captured by the employer through email monitoring. As we have mentioned in relation to information privacy, there is protection for information about third parties collected by the employer. However, as is the case for workers, there is limited privacy protection for third parties in relation to the implementation and use of the practices themselves.

## Conflicting Interests

3.107 The interests of third parties may also come into conflict with the privacy interests of workers. This conflict is apparent in the case of video surveillance

531 This is because the employee records exemption would not apply in these circumstances as there is no direct employment relationship between the third party and the worker. See Chapter 1, paras 1.22–1.24 for a discussion of the employee records exemption. If the third party does not record the information in some way, for example, if the third party only observes video monitors which are owned by the employer, then there is no 'collection' of information by the third party for the purposes of the Privacy Act, and the Act will not apply: *Privacy Act 1988* (Cth) s 16B.

532 Consultation 1.

533 Consultation 9.

534 Consultation 11.

535 See Chapter 2, paras 2.49, 2.71, and 2.91.

where both workers and third parties are captured on camera. Video surveillance is increasingly used in child care facilities to protect children from harm. Such video images not only capture the children, but also the child care workers. Unions told us video images from such surveillance can be streamed on to the Internet so parents can see their children are being appropriately cared for.[536] Schools are also increasingly using video surveillance around their grounds for security reasons. We were told in consultations that video surveillance could also be extended to aged care facilities. While there is an obvious need to protect children and the elderly from harm, the use of surveillance in these circumstances has the potential to impinge upon the privacy of the children and the elderly who are in care, as well as upon the workers who are caring for them.

3.108 One commentator argues that monitoring workers' computer activity could provide benefits to other groups, such as customers.[537] For example, patients' health data might be better protected by establishing audit trails to show who has viewed it. This necessarily means monitoring worker activity.[538] The privacy of one group (patients) may be at the expense of another (workers), but this may be justifiable in the circumstances.[539]

3.109 In this section we have described situations where the interests of third parties conflict with the privacy of workers. Circumstances concerning the interests of third parties raise complex workplace management issues which often extend beyond the scope of privacy concerns and so are beyond the scope of the Commission's terms of reference. The options which are proposed in the next chapter are confined to workplace privacy issues. These may indirectly address some of the issues that concern the privacy of third parties in the workplace.

## WORKER TO WORKER

3.110 While falling outside our definition of 'third parties', privacy issues can arise between workers. For instance, a worker could covertly take photos of another worker using a mobile phone camera within the workplace, or an IT help desk worker could pay particular attention to monitoring certain worker's personal emails. While these practices could invade the privacy of workers, we

536 Consultation 21.

537 Schulman, n 122, 53–4.

538 Ibid.

539 Ibid.

consider these issues as disciplinary matters that should be dealt with by the employer.

## THE CASE FOR REFORM

3.111 This chapter has revealed important concerns employers have in running and managing their businesses. It has also revealed the significant gaps that exist in the protection of workers' privacy in Victoria and the difficulties of taking third-party issues into account. It seems clear the status quo is not adequate in either protecting workers' privacy or addressing employer concerns.

3.112 If we accept that conceptually privacy is placed within a human rights framework, but it is not an absolute right, and that within the workplace differing expectations of privacy exist, we then need to determine how to resolve the issues identified. The current regulatory regime is unable to account for the particular environment within the workplace and fails to provide practical assistance to employers and workers in the onerous task of adequately balancing these issues.

3.113 We believe reform of this area is essential to provide the necessary regulatory guidance to both employers and workers, through mechanisms that allow for a proper evaluation and balancing of these complex interests. This is why reform to the status quo is required and why we advocate a new regulatory regime.

## CONCLUSION

3.114 Having identified the issues and gaps in protection in this chapter and proposed reform of the area by way of regulation, in the next chapter we outline some possible options for reform to address the gaps.

# Chapter 4
# Options for Reform

## INTRODUCTION

4.1 In the preceding chapter we outlined the key privacy issues associated with workplace surveillance, monitoring and testing that had emerged from our consultations with employer associations, employers and unions. We argued that the status quo is not adequate to protect workers' privacy and that law reform is required.

4.2 Chapter 3 revealed why employers use surveillance, monitoring and testing practices in running their businesses. Those reasons include protection of property, maintenance of security, selecting and measuring worker performance, reducing the risk of legal liability and evidence gathering. At the same time, workers were concerned about the potential of certain practices to compromise their autonomy and dignity in the workplace and to impact negatively on the relationship of trust between employers and employees. Added to this were the practical difficulties workers have in withholding their consent, the lack of transparency as to what and why practices were being used, the inaccuracy of certain practices in assessing suitability for work and the potential for discrimination resulting from the use of such practices.

4.3 Viewed as a whole, the central gap in protection seems to be the lack of regulation that enables the proper balancing of this complex set of interests. We recognise that, in the absence of such regulatory guidance, the weighing up of these interests in different contexts presents an extremely difficult task for employers and workers alike. Given this, the provision of an effective 'balancing mechanism' is the central premise from which we assess the following regulatory options.

4.4 The Commission's regulatory aim is not to prohibit practices, but rather to facilitate the balancing of issues identified. One employer put it succinctly—'employers don't need less regulation, but more targeted regulation'.[540]

4.5 In this chapter we review several kinds of regulatory models which we initially considered to regulate surveillance, monitoring and testing practices, but which we have not put forward as options. We outline the reasons for rejecting them and then go on to propose two broad options for reform. We describe how each of the options would operate, including the role the regulator would play and how the regime would be enforced. Before explaining the models we considered and describing the options for reform, we briefly address the issue of information privacy.

## INFORMATION PRIVACY

4.6 As we indicated in Chapter 1, we do not deal with information privacy in detail in this Paper.[541] However, the issue of information privacy is worthy of mention as the collection of information is an important result or consequence of the practices which we have described throughout this Paper.

4.7 As mentioned in Chapter 1, there is a significant gap in the protection of private sector employees' personal information due to the operation of the employee records exemption in the *Privacy Act 1988* (Cth).[542] The employee records exemption means the personal information of private sector employees is not protected by the National Privacy Principles in the Act.[543] One means of providing a minimum standard of information privacy protection to Victorian private sector workers might be to develop principles equivalent to the National Privacy Principles (excluding health information as it is already protected by the *Health Records Act 2001*). Such principles could be incorporated into the existing *Information Privacy Act 2000*.

---

540 Consultation 10.

541 See the discussion on information privacy in Chapter 1, paras 1.20–1.24.

542 The 'employee records exemption' is explained in Chapter 1 at paras 1.22–1.24.

543 The National Privacy Principles (NPPs) in Schedule 3 of the *Privacy Act 1988* (Cth) are principles which regulate the collection and handling of personal information about individuals by private sector organisations. The NPPs are as follows—NPP1: collection; NPP2: use and disclosure; NPP3: data quality; NPP4: data security; NPP5: openness; NPP6: access and correction; NPP7: identifiers; NPP8: anonymity; NPP9: transborder data flows; NPP10: sensitive information.

4.8 Such an approach would help to overcome some of the uncertainties and anomalies we have highlighted in relation to medical and psychological testing and the operation of the Health Records Act. This solution is not ideal as the personal information of private and public sector workers would still be treated differently.[544] But this approach would accord private sector workers minimum standards of information privacy protection and allow for their information privacy to be regulated consistently.

4.9 At the time of writing, the review of the employee records exemption in the Federal Privacy Act had not been completed. As we mentioned in Chapter 1, the Commission would prefer to await the outcome of that review before it considers making recommendations on information privacy for workers.

## GOALS IN DEVELOPING OPTIONS

4.10 The focus of this phase of the workplace privacy reference has been to consider what kind of law reform is required to protect workers' privacy in relation to workplace surveillance, monitoring and testing practices. In considering options for reform the Commission had three goals:

- to ensure minimum standards of privacy protection for workers without unduly limiting the ability of employers to run their businesses;
- to protect workers' privacy in a way that is sufficiently flexible to accommodate the needs of different workplaces; and
- to put in place mechanisms that ensure compliance with the selected regime.

4.11 The minimum standard of privacy protection should apply consistently to all workers including employees, independent contractors and volunteers.[545] A minimum standard does not mean workplace surveillance, monitoring and testing practices should be conducted in the same way in all circumstances. But it does mean the same factors should be taken into consideration before implementing any surveillance, monitoring or testing, no matter what the status of the worker (ie an employee, independent contractor, volunteer or other kind of worker).

544 The Information Privacy Principles (IPPs) in Schedule 1 of the *Information Privacy Act 2000* govern the handling of personal information by the Victorian public sector. They are similar, but not identical, to the NPPs in the *Privacy Act 1988*.

545 See Chapter 1 paras 1.4–1.7 for discussion of why all types of workers' privacy must be regulated.

4.12 The principle of flexibility recognises that privacy laws must take account of the differing circumstances existing within workplaces and the wide range of work relationships.

4.13 Any proposed regulatory model is found within a political environment 'which is intended to preserve the sometimes fragile balance between the interests of economic activity on the one hand and the public welfare on the other'.[546] The complexity of public policy, organisational behaviour and human nature is such that the achievement of regulatory objectives 'will usually not require a "magic bullet", but rather a combination of policy tools'.[547]

4.14 The regulatory approach the Commission proposes to adopt reflects this combination approach, focusing on the principles of the 'sanctions pyramid'.[548] The idea is that regulators move progressively up the pyramid, starting at the bottom with the persuasive approach which involves no sanctions (eg education, authorisations).[549] Where there is non-compliance, the regulator gradually progresses up the pyramid to the intermediate sanctions (eg compliance notices or warnings).[550] If non-compliance continues, the most severe sanction may be reached at the top of the pyramid (eg civil penalties).[551] Under this structure, the regulator is provided with a range of credible sanctions (with differing degrees of severity) that enables it to match the sanction to the particular form of non-compliance[552] in a proportionate manner.

## SOME APPROACHES CONSIDERED

4.15 In determining the type of law reform options to propose, the Commission initially considered and dismissed a number of approaches. Although there are aspects of these approaches which may be useful as part of a more

546 Keith Hawkins, *Environment and Enforcement: Regulation and the Social Definition of Pollution* (1984) 9.

547 Peter Grabosky, 'Regulation by Reward: On the Use of Incentives as Regulatory Instruments' (1995) 17 (3) *Law and Policy* 257 259.

548 John Braithwaite and Ian Ayres, *Responsive Regulation* (1992) 35.

549 Julia Black, 'Managing Discretion' (Paper presented at the ALRC Conference, Penalties: Policy, Principles and Practice in Government Regulation, 7 June 2001, Sydney) 18.

550 Ibid.

551 Ibid.

552 Ibid.

comprehensive model, of themselves they do not fulfil the three goals described above.

## ENCOURAGING EMPLOYERS TO RESPECT WORKERS' PRIVACY

### *BEST PRACTICE GUIDELINES AND EDUCATION*

4.16 We first considered a self-regulatory option involving the publication of best practice guidelines by a body such as the Victorian Privacy Commissioner on the implementation and use of surveillance, monitoring and testing practices by employers.[553] For example, there might be guidelines on implementing video surveillance, psychological testing, drug and alcohol testing and systems using biometric technologies. Employers would be encouraged to follow the guidelines but could ultimately choose whether or not they wished to do so.

4.17 This option would give employers flexibility in adapting the guidelines to suit their individual business needs. It would also overcome some employers' uncertainty by giving them guidance on how to implement the processes of surveillance, monitoring and testing. In this respect, education of employers and workers about their rights and responsibilities is important under any option for reform considered.

4.18 However, the main disadvantage of a model involving education and guidelines alone is that it would not provide a guaranteed minimum standard of privacy protection for workers. It would be solely left up to employers whether or not they wished to follow the guidelines.

### *INCENTIVES-BASED SCHEMES*

4.19 One way to encourage employers to follow best practice guidelines would be to offer them an incentive.[554] An example of an incentive-based approach would be making workplace privacy 'best practice' a requirement in tendering for government work.[555]

4.20 While this approach is flexible and more easily tailored to a diversity of workplaces, it has critical defects. First, not all businesses undertake work with

553 Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (1999) 39–41.

554 Ibid 41–42.

555 Ibid 46. This is also described as a 'market harnessing control'.

governments but the practices the reference covers can exist across all types of businesses. Secondly, this type of regulatory model does not designate breaches of workplace privacy as an unacceptable social practice, but instead leaves the issue to be determined by the economic priorities of each employer.[556] It can also be difficult to predict the effectiveness of such incentives 'on the ground'[557] as they do not provide minimum standards of workplace privacy protections. Consequently, there is no certainty for workers that their rights will be protected in the same way from workplace to workplace. Any transparency requirements, such as a written policy or notification, would be left to the employers' discretion to establish, rather than as a guaranteed part of workplace culture.

### *SANCTIONS INVOLVING REPUTATION*

4.21 Another type of model is to encourage compliance with best practice guidelines by imposing sanctions which affect an organisation's reputation.[558] Examples of such sanctions might be to disclose names of 'bad' employers in parliament or to require employers to publish apologies in the newspapers.[559]

4.22 This model, however, suffers similar difficulties to the incentive-based approach described above.[560] Unless bad workplace privacy practices are clearly stigmatised, it is unlikely such disclosures to parliament will have any real impact on a business. A parallel can be drawn with the reputation-based model contained in the *Equal Opportunity for Women in the Workplace Act 1999* (Cth) that requires companies to report to the regulator the number of women in management positions. The enforcement mechanism of the Act provides the regulator with the ability to name non-compliant employers in a report tabled before parliament.[561] The Equal Opportunity for Women in the Workplace Agency which administers the Act has reported in its 2003 census only a 0.4% increase between 2002 and 2003 in women holding executive management positions.[562] In fact, the number

556 Ibid 43.

557 Ibid.

558 Ibid 49–50. This is a form of 'disclosure' regulation.

559 Ibid.

560 Ibid 43–44.

561 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) ss 12, 19.

562 Equal Opportunity for Women in the Workplace Agency, *2003 Australian Census of Women Executive Managers* Fact Sheet .

of women in line to take on senior positions has dropped from 5% in 2002 to 4.5% in 2003.[563]

4.23 While the statistics generally show some limited improvement on past years,[564] overall there is considerable doubt about the effectiveness of this type of enforcement mechanism. The model allows for flexibility by simply requiring employers to submit a report on the features of their management program,[565] but it does not provide guaranteed minimum standards for women workers. Whilst the naming of an employer in a report tabled in parliament[566] could result in exclusion from tendering for Commonwealth Government contracts,[567] limitations exist with the tendering sanction (which have been outlined in paras 4.19–4.20). Under this enforcement mechanism, the agency does not have the power to instigate a general audit of employers to ensure compliance with their management program.[568] If the employer thinks the 'consequence' to its reputation will be negligible, then the behaviours that are supposed to be regulated will remain unchanged.

4.24 Furthermore, reputation-based models work best where consumers can 'vote with their feet' and give their business to another company on the basis of ethical considerations.[569] This does not translate so easily into a workplace privacy context. This is because it is highly unlikely job applicants and workers would have the luxury of rejecting jobs on the basis of undesirable workplace privacy

563 Ibid.

564 Ibid, where in 2003, 49.1% of companies had no women executive managers, down from 52.6% reported in 2002.

565 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 13.

566 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) ss 12, 19.

567 The agency's website states 'non-compliant employers may be affected by the Commonwealth Government Contract Compliance policy. The policy does not form part of the Act, but supports its implementation through two measures: (1) Commonwealth departments and agencies will not enter into contracts for the purchase of goods and services from non-compliant organisations; and (2) Employers that have been named in parliament for non-compliance with the Act will not be eligible for grants under specified industry assistance programs'. For further details and links to the Commonwealth Government's Contract Compliance Policy see: <www.eowa.gov.au/Reporting_And_Compliance/Complying_with_the_Act/Sanctions_for_not_Complying/Contract_Compliance_Policy.asp>.

568 We have been informed by the Equal Opportunity for Women in the Workplace Agency that an agency representative may visit an employer's site for audit-type purposes usually only when the employer has applied for a waiver from the reporting requirement pursuant to s 13C of the *Equal Opportunity for Women in the Workplace Act 1999* (Cth).

569 Baldwin and Cave, n 553, 49–50.

practices. Accordingly, this kind of approach on its own would not be effective in the workplace context, though it might be a useful approach when combined with other enforcement techniques.

### REGULATION OF PROVIDERS

4.25 In Chapter 2 we outlined the differing regimes that currently regulate surveillance, monitoring and testing. In the case of testing we also described how the industries or professions that supply testing technologies and methodologies currently regulate these practices (eg the medical/psychology professions). Many problems and inconsistencies have been revealed within the existing legislative and self-regulatory regimes governing these practices. Although it is important to note these are areas in need of possible law reform, a number of the issues involved are not specific to workplace privacy and as such are beyond our terms of reference. Accordingly, we have not proposed reforms which directly regulate the providers of surveillance and monitoring technologies or the professions and industries involved in psychological, medical or alcohol and drug testing.

## POSSIBLE REFORM OPTIONS

4.26 Two options which the Commission proposes to regulate workplace surveillance, monitoring and testing practices are:

> **Option 1**: A separate Act that would require employers to seek authorisation in advance from a regulator before undertaking either some or all surveillance, monitoring or testing practices in the workplace.
>
> **Option 2**: A separate Act that would require employers to comply with a set of principles on how they implement and conduct workplace surveillance, monitoring and testing.

4.27 Both options would achieve the three goals described above—that is minimum standards, flexibility and enforcement—but in different ways and to different degrees. Broadly, Option 1 would require the authorisation of all or some workplace surveillance, monitoring and testing practices before they are implemented in the workplace. Option 2 would require employers to comply with certain principles in instituting and applying such practices. Option 1 would have some resource implications and, depending on the use of practices, some compliance costs for employers. But it would provide greater certainty about acceptable and unacceptable practices for employers and workers than Option 2. Option 2 would put more direct responsibility on employers and may have less

resource implications for government. We outline the options in more detail below.

## OPTION 1—AUTHORISATION IN ADVANCE

4.28 This option proposes a new Act to regulate the practices of workplace surveillance, monitoring and testing. The core protection in the Act would be that the privacy of workers can only be restricted where some or all of those practices are appropriately authorised.

4.29 The key feature of the Act would be that employers would be required to seek written authorisation from a regulator before conducting some or all types of overt and covert surveillance, monitoring or testing in the workplace. The Act could also contain provisions limiting the use of covert practices (for example, use of hidden cameras) to specified situations.

4.30 Other features of this option could include:

- a process for notifying workers that an application for authorisation has been submitted to the regulator;
- a process for workers to be consulted about the application (either by the regulator or the employer);
- powers for the regulator to conciliate or hear disputes about the application between the employer and workers;
- powers for the regulator to enforce the Act and the conditions of authorisations by having the ability to audit employers and to issue compliance notices;
- an educative role to be fulfilled by the regulator; and
- removal of workplace surveillance issues from the *Surveillance Devices Act 1999*.

### ? QUESTION(S)

1. Should employers be required to seek authorisation from a regulator before conducting workplace surveillance, monitoring and testing? If so, what issues should be considered by the regulator in determining whether to authorise the use of these practices?

### *THE AUTHORISATION PROCESS*

4.31 The role of determining whether a practice is justified in the circumstances would fall to the regulator.

4.32 The employer would seek authorisation by means of a written application submitted to the regulator. In the application, the employer would be required to address issues such as:

- The nature of the practice (eg whether it is overt video surveillance, email and Internet monitoring, or psychological testing).
- The purpose of the practice (eg whether to detect theft, protect staff working in isolated locations, or improve productivity).
- The intrusiveness of the proposed practice (eg how many workers does it affect? In what circumstances are the workers affected? Does it involve continuous or random monitoring?).
- Whether there are less intrusive methods of achieving the required outcome (eg could extra supervision be used? Could the employer measure the worker's productive output rather than use monitoring? Has the employer given any such alternatives sufficient consideration?).
- The adequacy of consultations with workers where the employer wishes to use an overt practice.
- The reliability of the technology to be used.
- The adequacy of safeguards to ensure the practice is carried out appropriately (eg are the personnel who will be conducting the practice sufficiently qualified/senior/accountable?).
- The appropriateness of the timeframe (eg is the practice for a limited period? If it is being used for a longer period, is that justified and reasonable?).

4.33 Employers could either submit applications themselves or, if a practice is an industry-wide one, an employer association or industry body could submit the application on behalf of its members. For example, the Australian Retailers Association could submit an application on behalf of its members who use video surveillance. All Association members would be bound by the conditions of the authorisation when using video surveillance in their stores.

**? QUESTION(S)**

2. Are there any practical difficulties with the concept of industry-wide authorisations?

4.34 The Act could also contain a process to 'fast track' urgent applications. This would assist, for example, an employer with a strong suspicion a worker is committing an unlawful act such as fraud and fears evidence will be lost if authorisation for covert surveillance or monitoring is delayed. In such limited and extreme cases, the employer could seek an authorisation after the event, or the regulator could assess an urgent application on an expedited basis.

4.35 A similar 'authorisation in advance' model exists in France, where the law requires work rules[570] to be submitted to a state-appointed labour inspector for approval.[571] The inspector assesses the rules 'according to the laws and regulations in force and, where necessary, can order their modification or withdrawal'.[572] An employer who disputes the inspector's interpretation of the law may challenge it in court. Additionally, under French law an employer contemplating the installation

570 See *'France: Works Rules'* European Foundation for the Improvement of Living and Working Conditions which describes 'works rules' as a document 'setting down rules on health, safety and discipline within the enterprise which is a compulsory requirement in enterprises normally employing 20 or more employees. Under French law, the authority to set these rules lies with the employer, after consultation with the works council. Only in exceptional cases are they contained in a collective agreement. The legality of works rules is monitored by the labour inspector, who may at any time demand the withdrawal or amendment of an illegal provision. The law specifies, in outline, the manner in which works rules must accommodate the protection of individual and collective rights and freedoms. This is an area which gives rise to numerous matters of dispute'. A 'works council' is an institution of employee representation possessing legal personality and is a collegiate body composed not only of employee members elected by the workforce but also the head of the enterprise (who chairs the council and takes part in certain votes) and of representatives appointed by the trade unions (who act in a purely consultative capacity). It has charge of company welfare and cultural facilities, and the law invests it only with consultative powers in regard to employer initiatives concerning the organisation and management of the enterprise. It possesses no formal bargaining power. In practice, the dividing line between consultation, which is the prerogative of the works council, and collective bargaining, which is the prerogative of the representative trade unions, is a fine one. Numerous agreements, formal or otherwise, are concluded between the head of the enterprise and the works council, and the courts accord these certain legal force, at the least as unilateral undertakings on the part of the employer—see *'France: Works Council'* European Foundation for the Improvement of Living and Working Conditions .

571 Craig, n 412, 92.

572 Ibid 108.

of a workplace electronic monitoring system to enforce a 'works rule' could be required to:

- negotiate with its union over the system;
- inform and consult its works council about the system;
- seek approval for the proposed works rule and the associated system from the labour inspector; and
- register the system with the Commission Nationale de l'Informatique et des Libertes.[573]

4.36 In New South Wales, the *Workplace Video Surveillance Act 1998* contains an authorisation mechanism for employers who want to carry out covert video surveillance of employees in the workplace.[574] The Act prohibits an employer from carrying out covert video surveillance unless it is authorised by a magistrate and is solely for the purpose of establishing whether an employee is involved in unlawful activity in the workplace.[575] A covert surveillance authority does not authorise an employer to film employees in change rooms, toilets and bathing and shower facilities.[576] Nor does it authorise the use of covert video surveillance to monitor an employee's work performance.[577]

---

573 Ibid 108.

574 Under the Act, video surveillance is covert unless (a) employees have been notified in writing at least 14 days prior to the intended surveillance, (b) the video cameras used are clearly visible, and (c) signs notify people they are under surveillance and are clearly visible at each entrance to that part of the workplace in which surveillance is taking place: s 4(1). Additionally, video surveillance is not covert if employees have agreed to video surveillance in the workplace for purposes other than surveillance of the activities of employees and it is carried out in accordance with that agreement: s 4(2). Employees are taken to have agreed to the intended use of the surveillance if a body representing a substantial number has agreed on their behalf, and in the case of a new employee, who has been employed less than 14 days before the intended use of the surveillance, if the employee is notified in writing of the surveillance before commencing work: s 4(3). The Act does not require that 'overt' surveillance by employers be authorised.

575 *Workplace Video Surveillance Act 1998* (NSW) s 7(1) and part 3. Employers who use covert video surveillance without a covert surveillance authority have a defence against prosecution under s 7(1) if (a) the covert video surveillance was carried out solely to ensure the security of the workplace, and (b) there was a real and significant likelihood that the security of the workplace would be jeopardised if the covert video surveillance was not carried out: s 7(3).

576 *Workplace Video Surveillance Act 1998* (NSW) s 9(3)(b).

577 *Workplace Video Surveillance Act 1998* (NSW) s 9(3)(a).

4.37 The authorisation procedure requires the employer (or employer's representative) to apply to a magistrate for a covert surveillance authority. The application must include the following information:

- the grounds the employer has for suspecting employees are involved in unlawful activity;
- whether other managerial or investigative procedures have been undertaken to detect the unlawful activity and what has been the outcome;
- who and what will be in view of the cameras;
- the dates and times during which the covert surveillance will be conducted; and
- if the application is made by an employer's representative, verification acceptable to the magistrate of the representative's authority to act on behalf of the employer.[578]

4.38 The application must also nominate a licensed security operator who will oversee the conduct of the covert video surveillance operation.[579] If the authority is granted, it is granted upon the condition that the nominated security operator will oversee the covert video surveillance.[580]

4.39 In considering the application, the magistrate must have regard to whether covert video surveillance of the employees concerned might unduly intrude on their privacy or the privacy of any other person.[581] If the application potentially involves covert surveillance in an area where employees are not directly engaged in work, such as a meal or recreation area, the magistrate must have regard to employees' heightened expectations of privacy in that area.[582] The magistrate must not issue a covert surveillance authority unless the magistrate is satisfied the application shows there are reasonable grounds to justify its issue.[583]

578 Section 10(2).

579 Section 10(3).

580 Section 9(2).

581 Section 14.

582 Section 13(2)(a).

583 Section 13(1).

4.40 The exposure draft of the Workplace Surveillance Bill 2004 (NSW) which the New South Wales Government has recently issued, contains similar provisions in relation to applications for covert surveillance authorities.[584]

4.41 Another example of an authorisation process is contained in the *Trade Practices Act 1974* (Cth). Under that Act, corporations may apply to the Australian Competition and Consumer Commission (ACCC) to seek authorisation for conduct which might otherwise breach the Act's restrictive trade practices provisions.[585] The ACCC may grant an authorisation if the proposed conduct results in a benefit to the public which outweighs the detriment to the public of a lessening of competition.[586]

## ? QUESTION(S)

3. Are there any surveillance, monitoring or testing practices which should be permitted without authorisation? If so, which ones and why?

4. Should overt and covert practices be treated differently? If so, why?

### *THE NOTIFICATION OF WORKERS*

4.42 The Act would require employers to notify workers when an application for authorisation of a surveillance, monitoring or testing practice is submitted to the regulator. Certain covert practice applications would be the exception to the general notification requirement.

4.43 Notification could be provided to the entire workforce, or just the affected workers if they could be easily identified. For example, if an employer wanted to conduct alcohol and drug testing on a clearly identified group of workers, then only that group would need to be notified. Notification could be effected in a number of ways. One option could be to post a copy of the relevant application on a prominent noticeboard and make it clear to workers that they (or their representatives) can make a submission to the regulator. Another might be to

584 See particularly part 3 of the exposure draft of the Workplace Surveillance Bill 2004 (NSW) in relation to covert surveillance authorities. See n 4 for more information on the objects of the draft Bill.

585 See *Trade Practices Act 1974* (Cth) s 88.

586 See *Trade Practices Act 1974* (Cth) s 90.

notify affected workers (if they can be identified) directly in writing. A possible disadvantage of this approach is that it may result in employers preferring to use covert surveillance.

4.44 Apart from notification, workers' involvement may include submissions to the regulator. Alternatively, the regulator could have the power to seek submissions directly from workers. It could be a formal requirement of the authorisation process that the regulator (or employer) consult with workers about the application.

**? QUESTION(S)**

5. Should there be a mechanism to ensure proper consultation or communication with workers during the authorisation process? What is the best way to do this?

6. How can such a procedure be made effective, given the imbalance of power that may exist between an employer and workers?

### *THE REGULATOR'S ROLE IN THE AUTHORISATION PROCESS*

4.45 The regulator's role would be to assess applications for authorisation. The Commission envisages the regulator producing and publishing guidelines[587] on how it assesses each of the criteria. The regulator would assess each application on its merits, balancing each of the factors described in the application.

4.46 In assessing the application, the regulator should consider whether the use of the practice is reasonable in the circumstances, having regard to factors such as:

- Whether the use of the practice is proportionate to the risk involved (this requires a balancing of the purpose and effect of the privacy infringement).[588]
- Whether it is reasonable and practical for the employer to use a less privacy invasive practice.
- Whether proper consultation has occurred with workers.

587 This raises the potential issue that the development of guidelines may be based on existing Australian Standards (produced by Standards Australia).

588 Refer to Issues Paper, para 5.7, for a discussion of 'proportionality'.

- The nature of any objections raised by workers in response to the application.

4.47 The regulator could have the power to resolve disputes about applications. This could be achieved through a conciliation process, with the option of a hearing if the regulator thinks it necessary.

4.48 The Act could also include an appeals process if the employer or workers (or workers' representatives) were dissatisfied with the outcome of a hearing.

4.49 If the regulator is satisfied with the application, an authorisation to undertake the practice would be granted. Any conditions would be included in the terms of the authorisation, including the duration of the authorisation.

**? QUESTION(S)**

7. Would it be more appropriate for a court to assess authorisation applications than a regulator?

8. Is the proposed test to be used by the regulator that a practice is 'reasonable in the circumstances' an appropriate one?

### *ENFORCEMENT*

4.50 The regulator would also be responsible for enforcing the Act. Following the principles of the 'sanctions pyramid' (see paragraph 4.14), the key enforcement mechanisms under this option would be:

- a complaints-based mechanism;
- audit/investigation of employers' practices; and
- penalties for non-compliance.

4.51 Individuals could make a complaint to the regulator if, for example, they believed their employer had implemented a practice without seeking authorisation or was not complying with the terms of an authorisation.

4.52 The Act might provide that where two or more workers are affected by a practice that may breach the Act, any one of those individuals, or a representative organisation, could instigate a complaint about the practice on behalf of all the affected workers. Some existing information privacy legislation makes provision

for representative complaints (ie where one individual can instigate a complaint on behalf of others).[589] Similar provisions could be included in the new Act.

4.53 The Act would provide the regulator with powers to resolve complaints. This might be through a conciliation process similar to that which exists under the Health Records Act and the Information Privacy Act.[590] Under this model, complaints that are not resolved by conciliation are referred to a tribunal such as the Victorian Civil and Administrative Tribunal (VCAT). Alternatively, the Act could provide that the regulator investigate the complaint. The regulator could have the power to issue a determination[591] requiring the employer to remedy a breach, that compensation be awarded, or that the penalty for a breach be paid to the worker or workers concerned. The Act might need to include a mechanism for the regulator to assess compensation in circumstances where only one worker complains but a group of workers is affected.

**? QUESTION(S)**

9. What is the preferred method of handling complaints—conciliation or direct investigation by the regulator, or some element of both?

4.54 The regulator would also have powers of enforcement that do not depend on the trigger of an individual complaint. These powers would be exercised in a

589 See for example, *Privacy Act 1988* (Cth) ss 36(2), 38–39, *Information Privacy Act 2000* s 25(3), *Health Records Act 2001* s 45(3). Under the P*rivacy Act 1988* (Cth), individual complaints can become representative complaints when certain conditions exist. These conditions are: (a) the class members have complaints against the same person, (b) all the complaints relate to the same or similar circumstances, and (c) all the complaints give rise to a substantial common issue of law or fact: s 38(1). A representative complaint may be lodged without the consent of all the class members: s 38(3). Compare to s 45(3) of the *Health Records Act 2001* and s 25(3) of the *Information Privacy Act 2000* that require the consent of the individuals on whose behalf the complaint is made.

590 See for example, s 33(1) of the *Information Privacy Act 2000* which provides that if the Privacy Commissioner considers it reasonably possible that a complaint may be conciliated successfully, he or she must make all reasonable endeavours to conciliate the complaint. The Commissioner has powers to require a party, either personally or by representative, to attend a conciliation: s 33(3); and to require parties to answer questions or produce documents relevant to the complaint: s 34(1)(2). If conciliation fails, the matter may be referred to VCAT for hearing: s 37. See also the *Health Records Act 2001* ss 59–63 which contain similar provisions on conciliation.

591 See for example, *Privacy Act 1988* (Cth) s 52, which provides that the Federal Privacy Commissioner has the power to make determinations.

manner that enables the regulator to match sanctions to the particular form of non-compliance in a proportionate manner.

4.55 The first of these powers could be the ability to audit and investigate. If the regulator had reason to believe an employer was not following the terms of its authorisation, then the regulator could investigate the employer's practices. An audit could also be initiated by a worker's complaint.

4.56 The regulator could also have the power to randomly audit employers that are subject to an authorisation to ensure compliance. It could have the power to investigate matters on its own initiative where it believes a particular practice may be breaching the Act and it is in the public interest to investigate.[592] The regulator could also have powers to investigate systemic or industry-wide issues.

## ? QUESTION(S)

10. In your experience of other jurisdictions where the regulator has an inspectorate (such as OHS), how effective is the inspectorate model?

11. What level and kinds of penalties should there be for breaches of the Act?

4.57 In addition to these mechanisms, the regulator would have the power to issue compliance notices for breaches of the Act or any authorisation issued. The Act could provide that compliance notices be issued at the regulator's own initiative as well as in response to a complaint.[593] Compliance notices would set out what an employer has to do to remedy a breach. Failure to comply with a compliance notice would attract a penalty.

592 There is a similar provision in the *Privacy Act 1988* (Cth) s 40(2), which provides that the Federal Privacy Commissioner may investigate an act or practice that is an interference with the privacy of an individual, and the Commissioner thinks it is desirable that the act or practice be investigated.

593 For example, see the *Health Records Act 2001* which gives the Health Services Commissioner the power to issue compliance notices where an organisation has engaged in an act or practice that is a serious or flagrant contravention of the Act, or that has been engaged in at least five times within the past two years: s 66(1). The Health Services Commissioner may issue such a compliance notice on his or her own initiative or on application of a complainant whose complaint was subject to a conciliation agreement or determined by VCAT: s 66(5). See also ss 44(1)(5) of the *Information Privacy Act 2000* which give similar powers to the Victorian Privacy Commissioner.

4.58 We envisage the Act would provide for some lead time of about 12 months to give employers time to review their workplace surveillance, monitoring and testing practices and apply for relevant authorisations. Employers would not be penalised if they used surveillance, monitoring or testing during this period without an authorisation.

**? QUESTION(S)**

12. Is this enforcement regime appropriate? Are there any other mechanisms for enforcement that should be considered?

13. Should there be some lead time before the authorisation process applies?

### *EDUCATIVE FUNCTION*

4.59 Besides enforcement functions, the regulator's role would be to raise public awareness of the operation of the Act and to educate workers about their rights and responsibilities under it. Included in this role could be the preparation and publishing of publicly available guidelines which outline how the regulator assesses applications.

4.60 The regulator could also have an advisory role, assisting organisations to comply with the Act.[594]

## OPTION 2—GENERAL PRINCIPLES

4.61 This option proposes a new Act which would contain principles which employers would be required to follow when implementing workplace surveillance, monitoring or testing. The principles would be general in nature and address matters such as the purpose a practice is used for and communication with workers about the practice. This is similar to the information privacy legislation approach, although the information privacy principles are more detailed than the principles proposed under this option. Other features of this option could include:

- a code or codes[595] produced by the regulator (or an equivalent developed by industry and approved by the regulator) to provide practical details on

594 See Chris Maxwell, *Occupational Health and Safety Act Review* (2004), Chapter 25, para 1209 where Maxwell discusses the potential for conflict in the inspector's dual role of enforcement and giving advice.

how employers can comply with the principles in relation to particular practices—the codes would not be binding, but compliance with a code could be used by employers to defend themselves against worker complaints;

- powers for the regulator to conciliate or investigate complaints about breaches of the principles;
- powers for the regulator to issue compliance notices for serious breaches of the Act;
- an educative role to be fulfilled by the regulator; and
- removal of workplace surveillance issues from the *Surveillance Devices Act 1999*.

### *General Principles With Which an Employer Must Comply*

4.62 The Act would make employers responsible for the use and consequences of workplace surveillance, monitoring and testing. The Act could require employers to use these practices in accordance with principles, such as:[596]

- Surveillance, monitoring and testing must not be used in a way that breaches a worker's reasonable expectation of privacy.[597]
- Surveillance, monitoring and testing must only be undertaken for an acceptable purpose.
- Surveillance, monitoring and testing must be conducted in a fair manner and the use of the practice must be proportionate to the risk involved (this requires the balancing of the purpose and effect of the privacy infringement).
- Workers must be informed and consulted about the introduction and use of workplace surveillance, monitoring and testing.

595 The potential issue with reliance on Australian Standards for the development of such Codes is raised in n 587.

596 The principles are based on principles for undertaking overt surveillance recommended by the New South Wales Law Reform Commission, n 405,180–93.

597 See Chapter 1, para 1.18 on the issue of 'reasonable expectations of privacy'.

## ? QUESTION(S)

14. If legislation were enacted to introduce principles to govern workplace surveillance, monitoring and testing, what should those principles be?

### *CODES*

4.63 As the principles would be general in nature (so they could be applied to a variety of practices and workplaces) we envisage that codes of practice could be developed to provide practical assistance to employers. Codes could be developed for different types of practices. They could either be developed and issued by the regulator, or developed by industry and approved by the regulator. Codes would not have to be legally binding to be effective. Employers could use compliance with codes to defend themselves in the event of a worker's complaint that the employer had breached the Act's principles.

4.64 Information privacy regulators take a similar approach. They produce guidelines (rather than more formal codes of practice) to assist organisations to comply with information privacy principles. 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.[598] A similar approach is taken in the United Kingdom.[599]

4.65 The use of a code of practice as a defence is a regulatory method used in Victoria under the occupational health and safety regime.[600]

---

598 See Guidelines to the National Privacy Principles, September 2001 and Guidelines on Privacy in the Private Health Sector, October 2001, available at <www.privacy.gov.au> at 30 July 2004.

599 In the United Kingdom, employers are required to comply with the provisions of the Data Protection Act. 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 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, *The Employment Practices Data Protection Code: Part 3: Monitoring at Work* 6.

600 Under the Victorian occupational health and safety regime, compliance with codes is not mandatory. A person may choose to comply with the *Occupational Health and Safety Act 1985* and relevant Regulations in some other way, provided the requirements of the Act and the Regulations are fulfilled. A person cannot be prosecuted for failing to comply with an approved code of practice.

## ? QUESTION(S)

15. If codes are used to provide detail on complying with the general principles, should the codes be mandatory? Should they be used in some other way?

16. Has this model been effective in other jurisdictions?

### *COMMUNICATION WITH WORKERS*

4.66 We have suggested that this option includes a general principle which requires workers be informed and consulted about workplace surveillance, monitoring or testing. A code could put forward ways this might be achieved. For example, the code could suggest that the employer:

- outline how and why it intends to use the practice;
- outline the safeguards it will put in place to protect workers' privacy in relation to the implementation of the practice itself and the use and handling of any information collected; and
- put in place processes to give workers the opportunity to express their views about the practice.[601]

4.67 The code would not need to outline how communication and consultation takes place in specific circumstances. To allow for flexibility, this would be a matter for the particular workplace.

### *ENFORCEMENT AND EDUCATION*

4.68 Option 2 would again follow the sanctions pyramid approach set out in paragraph 4.14. It would contain a complaints-based regime which includes the same mechanism for making complaints as under Option 1. The difference between the two regimes would be that under Option 1, complaints would relate to authorisation of practices, whereas under Option 2, complaints would relate to a breach of the Act's principles.

---

However, failure to observe a relevant code can be used as evidence that a person has failed to comply with the Act or Regulations if the person has not adopted a credible alternative method of compliance: see *Occupational Health and Safety Act 1985* ss 55(8), 56. See also <www.workcover.vic.gov.au> at 30 July 2004 for more information about codes of practice.

601 These principles are based on principles suggested by Mr Chris Maxwell in relation to employer/employee consultation under the *Occupational Health and Safety Act 1985*. See Maxwell, n 594, Chapter 20, para 923.

4.69 The regulator would have the ability to issue compliance notices in Option 2, but unlike Option 1, it would have no audit powers. This would limit the regulator's ability to uncover matters which it could issue compliance notices about. Accordingly, the trigger for issuing a compliance notice under Option 2 would be either an individual worker's complaint or a representative complaint. A compliance notice could, for example, be issued if an employer did not comply with a determination issued by the regulator in response to a complaint. The regulator would also have an educative role similar to that outlined in Option 1.

## ADVANTAGES AND DISADVANTAGES OF THE OPTIONS

4.70 Options 1 and 2 fulfil our three goals for law reform to varying degrees. They also vary in the extent to which they address the gaps in the existing legal regime as outlined in Chapter 3. We examine the advantages and disadvantages of each option in light of these issues.

### *OPTION 1—AUTHORISATION IN ADVANCE*

#### Advantages

4.71 Under Option 1, the authorisation application would provide criteria against which the implementation of surveillance, monitoring and testing practices could be judged. This would have the effect of providing a set of minimum standards to protect workers' privacy in relation to those practices. Once the regulator had authorised a system, the employer would have to abide by the conditions of the authorisation. The conditions themselves would also provide a privacy protection safety net for workers.

4.72 The assessment of an authorisation application by the regulator provides an independent means of scrutiny of the employers' intended processes. The regulator would be more objective about the impact of the practice on workers' privacy than either the employer or the workers could be. On the other hand, employers may be concerned that a third party regulator would not know the employer's business and so could not readily judge whether an authorisation should be granted. Nevertheless, employers would have the opportunity to make their case for the use of a particular practice within the application.

4.73 Under this option, workers could have input into the authorisation process by making a submission to the regulator. However, there is no requirement under Option 1 that individual workers consent to the practice. Although this removes the difficulties associated with consent in the workplace which have been discussed in this Paper, in some circumstances workers might

want to have the opportunity to consent (or not to consent) to a particular practice. If consent were an issue in a particular case, a requirement for worker consent could be incorporated into the conditions of an authorisation.

4.74 Option 1 is flexible. In assessing an authorisation application, the regulator would be expected to take into account the nature of the employer's business, especially if a 'one size fits all' approach is not appropriate.

4.75 This option would provide a high level of certainty for both employers and workers. In the case of employers, if they received authorisation for their practice and complied with it, they could be confident their practice was lawful. Workers would also be certain about the conditions under which the employer could implement the practice. In addition, all workplace privacy obligations relating to practices would be located in one Act. The regulatory criteria and guidelines the regulator would be required to consider would provide employers with a 'one-stop-shop' on how to comply with the legislation.

4.76 The enforcement regime under Option 1 provides workers with a mechanism to make complaints about privacy breaches. This option does not rely on individual complaints to trigger action by the regulator (circumventing problems caused by the power imbalance between workers and employers—see Chapter 3, paragraph 3.60). The regulator would also have the ability to audit employers to check compliance with an authorisation. The regulator could have the power to investigate systemic issues that come to its attention.

4.77 The ability of the regulator to issue compliance notices would provide a mechanism for employers to remedy a breach of the Act themselves, before a penalty is imposed. However, a penalty could be imposed after an employer fails to comply with a compliance notice.

### Disadvantages

4.78 A potential disadvantage of Option 1 is that employers may see this model as placing onerous regulatory requirements on the way they conduct business. In particular, they may be concerned that it would inhibit their ability to retain a competitive edge. There would also be the compliance cost (both monetary and personnel) associated with the authorisation process. The employer would bear this cost regardless of the size of the business—no small business exemption is being proposed. However, it should be remembered that it is the employer alone who chooses which practices to implement in the workplace. Compliance costs only come with the decision to implement a surveillance, monitoring or testing practice. If employers do not wish to implement any practices, the compliance

cost would be nil. The model also allows for industry-wide authorisations which would significantly reduce the compliance costs of individual employers. It also provides for a regulator to issue the authorisation. This is a less costly and less formal alternative for employers than having to go to a court to obtain a covert surveillance authority, as required for covert surveillance in New South Wales.

4.79 Under this option, government funds would be required to extend an existing regulatory structure or create a new structure. The regulator would need resources to assess authorisation applications and cover the compliance process.

### *OPTION 2—GENERAL PRINCIPLES*

#### Advantages

4.80 Under Option 2, the requirement for employers to comply with the general principles in the Act would provide a safety net of minimum standards for workers who might be subject to surveillance, monitoring and testing in the workplace. From an employer's point of view, complying with general principles would make the option flexible as the application of the principles could be tailored to suit an employer's requirements. The option would also be less onerous for employers because they would not have to seek prior authorisation before implementing practices in the workplace.

4.81 Although the general nature of the principles would make Option 2 flexible, this is at the expense of certainty. Workers and employers might not be sure about their rights and obligations under the Act. For example, employers might find it difficult to apply the principles in practice. However, the production of codes on specific workplace practices would provide some of the practical details about how a surveillance, monitoring or testing practice might be implemented. This would help give employers and workers more certainty about their rights and obligations.

#### Disadvantages

4.82 The greatest disadvantage of Option 2 lies in the area of workers' privacy protection and enforceability. The codes the regulator (or industry) produces to explain how the principles operate would not be directly enforceable. Instead, the code only gives employers an incentive to comply because it could be used as a defence to a complaint. If employers do not perceive the risk of a complaint being high, there is nothing compelling them to comply with the code.

4.83 The other disadvantage in relation to enforcement is the reliance on a worker's complaint as the key trigger for the regulator to intervene in a matter.

This is because there is a power imbalance between workers and employers. Workers might be afraid they will jeopardise their position if they 'rock the boat'.[602] In its submission to the Issues Paper, the Equal Opportunity Commission Victoria (EOCV) noted that, from its experience of complaints processes, many workplace victims of discrimination, harassment and vilification suffer from victimisation as a result of lodging a complaint. The EOCV said any workplace privacy scheme that is introduced should consider the inherent limitations of a complaints-based system and consider alternatives to that system where appropriate. It noted this is particularly critical given that a worker complaining about a breach of privacy would be challenging their employer in the same way as in a discrimination complaint.

4.84 As for Option 1, if workplace surveillance was carved out of the *Surveillance Devices Act 1999*, the requirement for workers to consent to workplace surveillance would be removed. We mentioned above that under Option 1, the issue of consent could be addressed in an authorisation (see paragraph 4.73). Under Option 2 there is no mechanism to address consent issues. A consent requirement might be included as part of a code. It is unlikely this would provide workers with the same level of comfort as dealing with consent in an authorisation. Removing workplace surveillance from the Surveillance Devices Act would also remove the existing enforcement regime and criminal penalties currently associated with unlawful use of surveillance.[603] This means workers would have less protection from surveillance than they currently have.

## THE COMMISSION SEEKS YOUR VIEWS

4.85 The Commission is interested in responses to the questions posed in this chapter as well as any other comments or feedback on the options presented.

### ? QUESTION(S)

17. Have the advantages and disadvantages of Options 1 and 2 been adequately identified?

602 Submission 22.

603 See *Surveillance Devices Act 1999* ss 6(1), 7(1), 8(1), 11(1).

## ? QUESTION(S)

18. Do you prefer the option requiring 'authorisation in advance' or the option incorporating general principles? Explain your preference.

19. Would you prefer an option that combines aspects of each option? If so, which parts of each? Would you prefer a different option?

# Appendix 1

## LIST OF SUBMISSIONS RECEIVED

| No | Name | Affiliation |
|---|---|---|
| 1 | Brian Boyd | Victorian Trades Hall Council |
| 2 | Simon Moss | Australian Honesty Forum, Monash University |
| 3 | D Hughes | |
| 4 | Therese Dennis | |
| 5 | Alan Barron | |
| 6 | Peter Knowles | Victorian Transport Association |
| 7 | Edgar Didjurgies | International Power Hazelwood |
| 8 | Louise Russell | |
| 9 | Anonymous | |
| 10 | Andrej Kocis | Telstra Corporation Limited |
| 11 | Julie Mills | Recruitment @ Consulting Association Ltd |
| 12 | Kate Rattigan | Conduct & Ethics Unit—Office of Departmental Services |
| 13 | Murray Smith | Leader Community Newspaper |
| 14 | Dave Oliver | Australian Manufacturing Workers' Union |
| 15 | Lindy Smith | Australian Privacy Foundation |
| 16 | Paul Begley | Australian Human Resources Institute |
| 17 | Trevor Kerr | Southern Health Pathology |
| 18 | Gwynn Boyd | Minorplanet Asia Pacific Pty Ltd |
| 19 | **Confidential** | |
| 20 | John Mc Ginness | Commonwealth Attorney-General's Department |
| 21 | Peter Sanader | TTOTR (The Tout, On Track & Ratings) |
| 22 | Diane Sisely | Equal Opportunity Commission Victoria |
| 23 | Mervyn K Vogt | |
| 24 | Dan Romanis | Royal District Nursing Service |
| 25 | John Rush | The Victorian Bar |

| No | Name | Affiliation |
|---|---|---|
| 26 | Ian Gilbert | Australian Bankers' Association |
| 27 | Margaret Otlowski | Faculty of Law—University of Tasmania |
| 28 | Elizabeth Hayes | Victorian Automobile Chamber of Commerce |
| 29 | Helen Versey | Office of the Victorian Privacy Commission |
| 30 | Julie Phillips | |
| 31 | Christine Nixon | Victoria Police |
| 32 | Anonymous | |
| 33 | Eileen Tubb | |
| 34 | Alan Dudderidge | Transport Watchhousing Industry |

# Appendix 2

## CONSULTATIONS

1. Email and internet monitoring—technical expert, 20 October 2003
2. Psychological testing—technical experts, 20 October 2003
3. Biometrics and surveillance—technical experts, 22 October 2003
4. Testing and surveillance—union, 22 October 2003
5. Surveillance—employer associations and employer, 23 October 2003
6. Surveillance—unions, 23 October 2003
7. Email and internet monitoring—employer associations and employers, 24 October 2003
8. Email and internet monitoring—unions, 24 October 2003
9. Alcohol, drug and medical testing—technical experts, 31 October 2003
10. Testing—employer associations and employers, 5 November 2003
11. Testing—unions, 5 November 2003
12. Surveillance—unions, 11 November 2003
13. Testing—employer associations, 12 November 2003
14. Email and internet monitoring—employer, 14 November 2003
15. Email and internet monitoring—union, 18 November 2003
16. Surveillance, monitoring and testing—employer, 19 November 2003
17. Surveillance and testing—employer, 20 November 2003
18. Surveillance—employer association, 20 November 2003
19. Testing—union, 21 November 2003
20. Testing—employer, 21 November 2003
21. Testing and surveillance—union, 24 November 2003

# Appendix 3

## EMPLOYER ASSOCIATIONS, EMPLOYERS AND UNIONS CONSULTED

Association of Professional Engineers, Scientists and Managers, Australia
Australian Chamber of Commerce and Industry
Australian Childcare Centres Association
Australian Council of Trade Unions
Australian Education Union
Australian Human Resources Institute
Australian Industry Group
Australian Manufacturing Workers' Union
Australian Retailers Association Victoria
Australian Services Union
AXA – Asia Pacific Holdings Limited
Baulderstone Hornibrook
BHP Billiton Limited
Civil Air—The Australian Air Traffic Control Association
Coles Myer Ltd
Community and Public Sector Union
Electrical Trades Union of Australia (Southern States Branch)
Finance Sector Union
Liquor, Hospitality and Miscellaneous Union
Maritime Union of Australia
Multiplex Constructions
National Union of Workers
National Tertiary Education Union
Office of Public Employment
Shop, Distributive and Allied Employees' Association

Telstra Corporation Limited
The Australian Workers' Union
The Police Association (Victoria)
Transport Workers' Union of Australia
Transport Workers' Union (Vic/Tas Branch)
Victorian Automobile Chamber of Commerce
Victorian Employers' Chamber of Commerce and Industry
Victorian Farmers Federation
Victoria Police
Victorian Trades Hall Council
Victorian Transport Association

## TECHNICAL CONSULTATIONS

Mr Greg Acutt, Telstra Corporation Ltd
The Hon Terry Aulich, Aulich & Co
Dr Martin Boult, OSA Group
Mr Nick Carter, SHL
Mr Matthew Cox, a.g.e Enterprises
Mr Arthur Crook, Australian Psychological Society
Adjunct Professor Olaf Drummer, Victorian Institute of Forensic Medicine
Dr Ted Dunstone, Biometix
Dr Ian Freckelton, Barrister
Mr Victor Harcourt, Russell Kennedy Solicitors
Dr John Lewis, Pacific Laboratory Medical Services
Ms Dianne Lissner, Psychological Corporation (Aust & NZ)
Mr Les Newberry, CR Kennedy & Co Pty Ltd
Mr Jim O'Flynn, CR Kennedy & Co Pty Ltd
Mr Michael Pickering, Telstra Corporation Ltd
Ms Marian Power, Australian Council for Educational Research
Associate Professor David Suter
Mr Mike Thompson, Linus

# Appendix 4

## 1. SHORT ANSWERS TO QUESTIONS

### 1.1 Whether the Privacy Act 1988 (Cth) and/or the Workplace Relations Act 1996 (Cth) "cover the field" with respect to "employee records".

1.1.1 It is unlikely that either the *Privacy Act 1988* (Cth) or the *Workplace Relations Act 1996* (Cth) would be found to cover the field with respect to the information privacy aspects of the keeping of employee records. The provisions of these Commonwealth Acts, along with relevant extrinsic materials, indicate that neither legislative regime was intended as an exhaustive treatment of that subject. In particular, neither Act appears intended to exclude the States and Territories from regulating the privacy aspects of the keeping of employer records.

1.2 **Whether the existing Health Records Act 2001 (Vic) is capable of regulating health information of private sector employees or is invalid pursuant to s. 109 of the Constitution because it is inconsistent with either:**

**(a) *Privacy Act 1988* (Cth); and/or**

**(b) *Workplace Relations Act 1996* (Cth).**

1.2.1 As the *Privacy Act 1988* (Cth) does not cover the field of information privacy respecting employee records, and exempts those records from its regulatory scheme, the *Health Records Act 2001* (Vic) likely applies unhindered to the keeping of employee records. On the other hand, there is scope for inconsistency between the *Health Records Act 2001* (Vic) and the *Workplace Relations Act 1996* (Cth). Circumstances can be imagined in which an employer's obligations under the Commonwealth regime would conflict with the non-disclosure requirements of the Victorian regime. However, this "operational inconsistency" would only render the Victorian Act inoperative in the event, and to the extent, that such potential clashes actually did arise. In any case, the *Health Records Act 2001* (Vic) may not on its own terms operate in situations of potential conflict.

### 1.3 Whether the *Telecommunications (Interception) Act 1979* (Cth) "covers the field" with respect to "monitoring"?

1.3.1 There is strong authority for the view that the *Telecommunications (Interception) Act 1979* (Cth) exclusively covers the field of the 'interception of communications passing over a telecommunications system' as those

terms are defined in the Act. That authority seems to be well supported by an analysis of the provisions of the Act.

**1.4 Whether the *Surveillance Devices Act 1999* (Vic) is capable of regulating "monitoring" of private sector employee communications or is invalid pursuant to s 109 of the Constitution because it is inconsistent with the *Telecommunications (Interception) Act 1979* (Cth)?**

1.4.1 The *Telecommunications (Interception) Act 1979* (Cth) would not cover all the 'monitoring' activities that could be undertaken in relation to private sector employee communications. It is limited to the 'interception of communication passing over a telecommunications system' as those terms are defined in the Act. The *Surveillance Devices Act 1999* (Vic) is capable of regulating the monitoring of private sector communications that do not fall within that field. It will thus be important to identify the 'monitoring' activities not falling within the field occupied by the *Telecommunications (Interception) Act 1979* (Cth).

**1.5 Guidance on the constitutional implications of the various models by which workplace privacy might be regulated at the State level.**

1.5.1 We have provided some general observations at 3.6 below.

**2. SECTION 109 INCONSISTENCY – GENERAL PRINCIPLES**

2.1 As the Commission's briefing document notes, there are two established approaches to uncovering s 109 inconsistency. High Court authority in this area tends to talk about inconsistency as being either "direct" or "indirect". Direct inconsistency arises where provisions of State law operate to "qualify, impair … [or] negate" the intended operation of Commonwealth law: *Australian Mutual Provident Society v Goulden* (1986) 160 CLR 330 at 339; *Telstra Corporation Limited v Worthing* [1999] HCA 12 at [31]. Indirect inconsistency is typically analysed as a question of whether Commonwealth law "covers" a particular regulatory "field". Commonwealth provisions that seem "intended as a complete statement of the law governing a particular matter" will be taken to cover the field, so as to exclude State law from operating within that same field: *Victoria v The Commonwealth* (1937) 58 CLR 618 at 630 per Dixon J.

2.2 The Court has confirmed recently that the two approaches to identifying s 109 inconsistency are distinct and free-standing. In particular, findings that a Commonwealth law does not "cover the field" and that a State law occupies some very different field will not preclude a finding of direct inconsistency: *Telstra v Worthing* [1999] HCA 12 at [28].

2.3 Nevertheless, the Court accepts that the two tests are closely interrelated and can overlap in particular instances. As explained in *Ansett v Wardley*, the

tests represent alternate ways of gauging the Commonwealth Parliament's *intent* as to how, and by whom, particular matters will be regulated: *Ansett Transport Industries (Operations) Pty Ltd v Wardley* (1980) 142 CLR 237 at 260, 274, 280. When faced with a s 109 question the Court often frames the issues twice over, from each perspective, to obtain maximum guidance on that ultimate issue of Commonwealth intent.

2.4 Several of the High Court's recent decisions under s 109 have turned on the concept of "operational inconsistency". This kind of inconsistency arises where, in particular factual circumstances, Commonwealth and State legislative provisions cannot coexist comfortably – even though they might do so in other factual settings: *Victoria v The Commonwealth ("The Kakariki")* (1937) 58 CLR 618. An important feature of operational inconsistency is that the relevant State law will remain operative unless and until the circumstances of potential conflict actually do arise. Even then, the offending State law will only be rendered inoperative *in the particular factual circumstances* that bring it into conflict with Commonwealth provisions. Its operation in other circumstances will continue unhindered: *Commonwealth v Western Australia (Mining Act Case)* (1999) 196 CLR 392 at 417 [61]-[62], 439 [13]. In effect this allows only case-by-case assessment of inconsistency – a finding in one case need have no wider ramifications for the operation of the relevant State law.

## 3. DETAILED DISCUSSION

### 3.1 Whether the Privacy Act 1988 (Cth) and/or the Workplace Relations Act 1996 (Cth) "cover the field" with respect to "employee records".

*Privacy Act 1988* (Cth):

3.1.1 According to its long title, the *Privacy Act 1988* (Cth) ("the Privacy Act") is "An Act to make provision to protect the privacy of individuals". However, its provisions indicate that its field of operation is somewhat narrower, being confined to matters of "information privacy".

3.1.2 Section 3 of the Privacy Act, as amended by the *Privacy Amendment (Private Sector) Act 2000* (Cth) ("the Amendment Act"), negates any intention on the part of the Commonwealth to cover the entire field of information privacy.[604] The statement of purpose in s 3 of the Amendment Act, referring

604 Section 3 of the *Privacy Act 1988* (Cth), as amended by the *Privacy Amendment (Private Sector) Act 2000* (Cth), provides:

> It is the intention of the parliament that this Act is not to affect the operation of a law of a state or of a territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information (including such a law relating to credit reporting on the use of

to “a single comprehensive national scheme”, does not alter the overall impression as to intent. The National Privacy Principles, which presume an ongoing operation for State laws,[605] strengthen the view that the Commonwealth scheme is not intended entirely to cover the field of privacy protection.

3.1.3 The narrower question of the Commonwealth’s intention regarding regulation of employee records could be analysed in terms of an intention to cover that discrete sub-field. However, in keeping with the overlapping nature of the alternate inconsistency tests, the question may also be viewed as raising a particular shade of “direct” inconsistency. This analysis assumes that the Commonwealth has established a positive rule of "no regulation", which would then conflict directly with State attempts to regulate. The High Court often favours this approach where directing its inquiry to a narrow sub-set of a statute's broader regulatory field. The treatment of employee records within the Privacy Act regime is a narrowly cast issue that lends itself to direct inconsistency analysis.

3.1.4 Direct inconsistency under s 109 will arise where “a State law prohibits conduct permitted expressly or impliedly by a federal law”: *Wardley* at 275 per Aickin J. In terms of permitting conduct, a Commonwealth law can sometimes manifest an intention that some activity remain entirely free from regulation at all levels - a "no regulation" rule: *Botany Municipal Council v Federal Airports Corporation* (1992) 175 CLR 453. This differs from an intention that the activity be free from *Commonwealth* regulation. Intentions of the latter kind leave the way open for regulation at the State and Territory level.

3.1.5 Where the Commonwealth Parliament has not made its intention express, the Court must infer an intention as to the scope for concurrent State law. The Court asks whether State law on some particular matter would “qualify, impair … [or] negate” the intended operation of Commonwealth law: *AMP v Goulden* at 339; *Telstra v Worthing* at [31].

3.1.6 The Commission has requested advice as to whether the Privacy Act successfully monopolises the field of “employee records”. While that is an important question, we think the Commission may find value in a broader examination of the ways in which State legislation could operate in the gaps left by the Privacy Act. The entire scheme of exemptions is important, both from the perspective of a legislating State seeking to find gaps and from that

---

information held in connection with credit reporting) and is capable of operating concurrently with this Act.

605 NPP 2.1(g) (“use or disclosure … required or authorised by or under law”); NPP 6.1(h) (“denying access … required or authorised by or under law”). See also the Attorney-General’s Second Reading Speech in the House, 12 April 2000.

of a court asked to interpret the Privacy Act and resolve inconsistency questions.

3.1.7 The Privacy Act creates exemptions on two bases. First, it exempts some organisations altogether from compliance with its provisions, including small businesses, political parties and State and Territory authorities.[606] Second, the Privacy Act exempts from its operation some specific acts and practices engaged in by organisations. The keeping of "employee records" is one such exempt practice.[607] Notably, that exemption does not extend to disclosures not related to the employment relationship, nor to information held about prospective, rather than current or former, employees: Privacy Act s 7B(3).

3.1.8 As to exempt organisations, there is a strong probability that State legislation is able to fill those gaps without generating inconsistency. The total exclusion of the various exempt organisations from the Privacy Act's operation suggests strongly that their rights and obligations are to be left to the general law, rather than that they are intended to be free from all regulation: *Commonwealth v WA* (1999) 196 CLR 392 at 416-7 per Gleeson CJ and Gaudron J. This interpretation of the Act's provisions can be confirmed by reference to extrinsic materials. The *Acts Interpretation Act* 1901 (Cth) s 15AB(1)(a) permits courts to consider extrinsic materials "to confirm that the meaning of [a Commonwealth] provision is the ordinary meaning conveyed by the text of the provision taking into account its context in the Act and the purpose or object underlying the Act." Nothing in the available extrinsic materials suggests a Commonwealth intention that exempt organisations be immunised from all privacy-related regulation. For these reasons, State laws ought to be able to regulate the keeping of employee records by exempt organisations, including small businesses.

3.1.9 For exempt acts and practices, including employee records, the question is more finely balanced. It is not quite so self-evident here that the Commonwealth wanted simply to refrain from imposing its own layer of regulation. Rather, a respectable argument could be mounted that the Commonwealth intended a "no-regulation" regime for particular acts and practices, ruling out State and Territory regulation.[608]

3.1.10 Nevertheless, we think the better view is that the Commonwealth has left the way open for State and Territory regulation of exempt acts and practices, and of employee records in particular. Two very different considerations point

606 *Privacy Act* s 6C(1).

607 *Privacy Act* s 7B(3).

608 Justice Dixon in *Wenn v Attorney-General (Vic)* (1948) 77 CLR 84 at 120 described this as an "intention to legislate upon a subject exhaustively to the intent that the areas of liberty designedly left should not be closed up".

to that conclusion. First, the suggested interpretation results in both sets of exemptions in the Privacy Act receiving consistent treatment.[609] Second, the ordinary meaning of the language of the provisions – ie. that the exemption from regulation relates only to the Commonwealth regime – finds confirmation in relevant extrinsic materials. Those materials suggest a Commonwealth intention to *defer* making a firm decision on whether, and how, employee records ought to be regulated.[610] The Attorney-General's Second Reading Speech to the House observes that personal information in employee records is "deserving of privacy protection", though not via the Privacy Act.[611] He goes on to foreshadow a short-term formal review of that position, including consultation with stakeholders. This all seems consistent with an intention that the general law, including State and Territory laws, continue to apply to employee records while the Commonwealth contemplates its longer-term policy position.

3.1.11 The intention to leave room for the ongoing operation of State and Territory laws is also evident in the government's response to recommendations made by the House of Representatives Standing Committee on Legal and Constitutional Affairs regarding the 2000 Amendment Bill. That response stated:[612]

> The regulation of employee records is an area that intersects with a number of State and Territory laws on workplace relations, minimum employment conditions, workers' compensation and occupational health and safety, some of which already include provisions protecting the privacy of employee records. The government considers that the attempt to deal with employee records in the Bill might result in an unacceptable level of interference with those State and Territory laws and a confusing mosaic of obligations.

3.1.12 The question of the sufficiency of Commonwealth legislative power is relevant here, too. It provides a further reason for not finding in the Privacy Act an intention that employee records be entirely free of all regulation, including State and Territory regulation. The Privacy Act seems to have been

---

609 As a general rule of interpretation courts will assume, absent contrary indications, that an enacting parliament intended to achieve consistency within a regulatory scheme: *Project Blue Sky v Australian Broadcasting Authority* [1998] HCA 28 at [69]-[70] per McHugh, Gummow, Kirby, and Hayne JJ.

610 In particular, the Attorney-General's Second Reading Speech to the House on 12 April 2000, his media statement of 22 December 2000, and documents generated as part of the ongoing process of consultation and review there foreshadowed.

611 Daryl Williams MP, Second Reading Speech to the House, 12 April 2000.

612 Commonwealth of Australia, *Government Response, House of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, September 2000, p 4.

enacted principally in reliance upon the Commonwealth's s 51(xxix) external affairs power; the Act's preamble recites that Australia has made international commitments concerning the protection of privacy. However, provisions enacted in reliance upon the so-called "treaty aspect" of the external affairs power must, for validity, give effect to[613] the provisions of the relevant treaty or convention: *Victoria v Commonwealth (Industrial Relations Case)* (1996) 187 CLR 416. As Australia's international undertakings concern the *protection* of privacy, s 51(xxix) might not furnish the necessary legislative power to support a "no-regulation" rule immunising employee records from all privacy-related regulation. Nor would the s 51(xxxv) industrial relations power be enlivened in the absence of an interstate dispute. An array of other heads of Commonwealth legislative power could give partial and piecemeal effect to a no-regulation rule in some spheres. Nevertheless, the difficulty in sourcing legislative power to underpin a no-regulation rule is a further factor militating against that construction of the employee records exemption.

*Workplace Relations Act 1996* (Cth):

3.1.13 The employee records provisions within the *Workplace Relations Act 1996* (Cth) ("Workplace Relations Act") and the incorporated Regulations are tailored to a very narrow objective; they facilitate the process of documenting breaches of employer obligations.[614] Given that narrow focus, it is very unlikely that the provisions were intended as an exclusive and exhaustive statement of the law governing the keeping of records about employees.[615] Moreover, it is not clear that the Commonwealth would possess the necessary legislative power to enact a comprehensive regime covering all aspects of the keeping of employee records.[616] Accordingly, the employee

613 The precise test is whether Commonwealth provisions are "reasonably capable of being considered appropriate and adapted to implementing the treaty": *Victoria v Commonwealth (Industrial Relations Act Case)* (1996) 187 CLR 416 at 487 per Brennan CJ, Toohey, Gaudron, McHugh and Gummow JJ.

614 Explanatory Memorandum to the Industrial Relations Legislation Amendment Bill (No. 2) 1990 (Cth), page 8; Senator Robert Ray, Second Reading of the Industrial Relations Legislation Amendment Bill (No. 2) 1990 (Cth), House Hansard, 18 October 1990.

615 In *Woodside Energy Limited v McDonald* [2003] FCA 69 at [97], Carr J considered that s 285B of the Workplace Relations Act may, together with surrounding provisions, "cover the field" on the subject of union access to work sites. This is unlikely to impact upon the question of whether s 285B and accompanying Regulations cover other fields, such as the keeping of records concerning employees.

616 The current employee records provisions of the Workplace Relations Act have a clear connection to interstate industrial disputation, and so find support in s 51(xxxv) of the Constitution. The privacy aspects of record keeping by employers, unless made the subject of a dispute, seem unlikely to find support in s 51(xxxv). Other heads of Commonwealth legislative power might provide piecemeal coverage.

records provisions of the Workplace Relations Act do not enliven the principles of "cover the field" inconsistency.

3.1.14 Nor is the Commonwealth scheme suggestive of a narrower intention to exclude State and Territory laws dealing, in particular, with the privacy aspects of employer record-keeping. In other words, it does not seem that the Act intends to confer upon employers a positive authority to keep and deal with employee records free from any privacy-related restrictions that might otherwise be imposed by State law: *Botany Municipal Council v Federal Airports Corporation* (1992) 175 CLR 453 at 465.

3.1.15 The structure and language of the employee records provisions manifest a narrow concern with ensuring that certain records are *kept* and made *available* to interested parties. That this ordinary meaning accurately reflects the Commonwealth Parliament's intention can be confirmed by reference to relevant extrinsic materials. When the principal provision dealing with record keeping was enacted, the Explanatory Memorandum and Second Reading Speech emphasised a narrow legislative purpose of facilitating "identification and correction of award breaches".[617] Nothing in the provisions themselves or related extrinsic materials adverts to potential privacy issues relating to record keeping. Judicial consideration has focused upon the provisions' concern for the convenience and property rights of *employers.*[618]

3.1.16 The Attorney-General's statement in his Second Reading of the Privacy (Private Sector) Amendment Bill 2000 (Cth), that workplace relations legislation would be a more appropriate source of privacy controls over employee records, can have no bearing on the interpretation of the Workplace Relations Act. Views expressed after provisions have been enacted cannot be taken into account in ascertaining the meaning of those provisions: *Hunter Resources Ltd v Melville* (1988) 164 CLR 234 at 240-1 per Mason CJ and Gaudron J. In any case, even if the Attorney-General's views were admissible, they seem to acknowledge that the Workplace Relations Act does not at present govern privacy issues concerning the keeping of employee records.

3.1.17 State and Territory laws will, then, be able to regulate the privacy aspects of the keeping of employee records, except to the extent that they directly "alter, impair, or detract from the operation of" the Workplace Relations Act's

---

617 Senator Robert Ray, Second Reading of the Industrial Relations Legislation Amendment Bill (No. 2) 1990 (Cth), House Hansard, 18 October 1990. See also Explanatory Memorandum to the Industrial Relations Legislation Amendment Bill (No. 2) 1990 (Cth), page 8.

618 See *Australian Meat Industry Employees' Union v Australian Food Corporation Pty Ltd* [2001] FCA 1709 at [87] per Hill J, emphasising the limited nature of the right to inspect employee records by reason of the underlying occupier's rights of employers.

employee records provisions: *Telstra v Worthing*. There is clear potential for State laws to have such an impact. This is explained further in 3.2 below, with specific reference to the *Victorian Health Records Act* 2001 (Vic).

**3.2 Whether the existing Victorian Health Records Act 2001 (Vic) is capable of regulating health information of private sector employees or is invalid pursuant to s. 109 of the Constitution because it is inconsistent with either:**

**(a) *Privacy Act 1988* (Cth); and/or**

**(b) *Workplace Relations Act 1996* (Cth).**

*Privacy Act 1988* (Cth)

3.2.1 As explained at 3.1.2 above, the Privacy Act does not "cover the field" of information privacy. The *Victorian Health Records Act* 2001 (Vic) ("Health Records Act") will, then, continue to operate effectively except to the extent of any direct inconsistency. That kind of inconsistency arises where State law is found to "qualify, impair … [or] negate" the intended operation of Commonwealth law: *AMP v Goulden* at 339; *Telstra v Worthing* at [31].

3.2.2 Assuming that the Heath Records Act is found to apply to employee records, its provisions are unlikely to be inconsistent with the Privacy Act. As explained at 3.1.10 above, the Commonwealth's decision to exempt employee records from the Privacy Act's operation is best viewed as *not* evincing an intention that employee records be immunised from all privacy-oriented regulation at all levels. If this is correct, it is difficult to see how the operation of the Health Records Act could qualify, impair, or negate the Privacy Act regime. Accordingly, the Health Records Act's non-disclosure regime is likely to have full operation in the context of employee records.

3.2.3 At the very least, the Health Records Act clearly is able to regulate health information held by small business employers, and other "exempt organisations" (see 3.1.7, above). Although this avenue secures only partial coverage for the Health Records Act, that coverage will extend to a substantial number of employee records.

*Workplace Relations Act 1996* (Cth)

3.2.4 Unlike the Privacy Act, the Workplace Relations Act creates positive obligations regarding the keeping of employee records. There is, then, the potential for a direct collision between those obligations and obligations imposed under the Health Records Act. If there are situations in which an employer's observance of the Victorian provisions would impair or negate the functioning of the Commonwealth's rules as to record keeping, s 109 of the Constitution will be engaged. The provisions of the Health Records Act would, then, be rendered inoperative to the extent of their inconsistency with

provisions of the Workplace Relations Act. This would likely be analysed as a matter of "operational inconsistency", as explained at 2.4 above.

3.2.5 At least one scenario can be imagined in which the Health Records Act would likely prove operationally inconsistent with the Workplace Relations Act. The latter instructs employers to allow authorised inspectors and union officers to examine employee records when those records are "relevant to [a] suspected breach" of the employer's obligations: Workplace Relations Act s 285B(3)(a)(iii). On occasion, health information kept as part of an employee record would be relevant in this way.[619] For instance, an employee's record may contain medical certificates or other health information that would be relevant in establishing entitlements to sick leave or pay (Regs 131G, 131T). This kind of information clearly qualifies as health information as defined in s 6 of the Health Records Act, and when found in employee records is likely subject to the Act's non-disclosure rules.[620] If a case arose in which an inspector demanded access to those parts of a record, the Victorian law's instruction to withhold would directly contradict the Commonwealth law's instruction to disclose. The Victorian provisions would, then, be "operationally inconsistent" and so inoperative in the particular factual setting at issue.

3.2.6 Some employers may also choose, or be required under certified "comparable" arrangements (Regs 131P(1), 131PA(1)), to keep in employee records health information going beyond that specified in the Workplace Relations Act and Regulations. For example, this could include information about counselling, drug tests or treatment, or other health assessments that may be relevant to a contested suspension or dismissal. Nothing in the Act or Regulations suggests that this additional health information, once in a record, could not be compelled where "relevant" to a suspected breach.

3.2.7 Findings of operational inconsistency in these situations might, in any case, be sidestepped by arguing that the Health Records Act has no operation. For example, an employee whose health information was demanded under the Workplace Relations Act regime might be taken to have waived privacy rights under the Health Records Act, perhaps by making a complaint that prompted a union officer's demand: Health Privacy Principle 2.2(b). Alternately, and more generally, a request made under the Commonwealth regime to view a record may count as disclosure "required … under law",

619 The case of *CFMEU v Able Demolitions and Excavations Pty Ltd* [2000] FCA 1247 concerned a union officer's demand for access to employee records so as to establish, among other things, that the respondent employer was paying required disability allowances.

620 The Act was clearly intended to regulate health information held in employee records: Gould MP, Second Reading of the Victorian Health Records Bill 2001 (Vic), Legislative Council, 22 March 2001. In view of this, a court would likely find that the Act does so extend.

which is exempt from the Health Records Act's non-disclosure requirements: Health Privacy Principle 2.2(c). In a case where either argument was accepted, the Victorian Act's non-disclosure requirements would be inapplicable and so could not be found inconsistent with the Workplace Relations Act disclosure regime.

### 3.3 Subsidiary questions regarding the *Privacy Act* and the *Workplace Relations Act*

3.3.1 In addition to the main questions collected on page 1 of the Commission's briefing document, some further questions are posed at other points. We will deal with those here, to the extent that they relate to the Privacy Act and the Workplace Relations Act and have not been addressed already.

*Is there relevance in Victoria's referral of powers to the Commonwealth, per Workplace Relations Act s 497?*

3.3.2 As explained at 3.1.13 above, we consider that the Workplace Relations Act's employee records provisions are not intended to cover the field of workplace information privacy. For that reason, our opinion is that Victoria's referral of powers does not bear on the divining of "intentions" in the context of establishing s 109 inconsistency. The referral might, though, bear upon the Victorian Parliament's power itself to regulate other aspects of privacy in the workplace. Any new provisions purporting to deal with matters over which power has been referred would need to be drafted to ensure an effective claw back of power. It is unclear to what extent that referral would be construed to encompass matters of workplace privacy. However, such matters are not traditional subjects of award terms and conditions, so probably would not come within the scope of the referred powers, at least if new laws are drafted carefully with this issue in mind.

*What is the status of s 7 of the Health Records Act in the context of the Federal Acts?*

3.3.3 Section 7 of the Health Records Act does not impact upon that Act's interaction with Commonwealth law. Section 109 of the Constitution governs the relationship between State and Commonwealth provisions and intentions expressed in State law cannot condition s 109's operation. Moreover, the fact that a particular State law might cede or submit to other State laws has no bearing on an analysis of its consistency with Commonwealth law.

*Can the States legislate on the ability of employers to search, test, employees etc prior to either "collection" for the purposes of the Privacy Act or before such information is included as part of an "employee record" for the purposes of the Workplace Relations Act?*

3.3.4 The two sets of Commonwealth provisions, in their dealing with employee records, would not prevent States from regulating broader aspects of the

privacy of employees. This is because, as explained above, neither set of provisions covers that particular field. Thus, the fact that employer searches or tests might eventually give rise to an employee record will not, of itself, bar States from regulating those activities. However, other aspects of the regulatory schemes contained in the Privacy Act and the Workplace Relations Act do touch upon non-record related invasions of employees' privacy. There is at least the potential for some Commonwealth provisions to be inconsistent with State efforts to regulate the searching, testing, etc, of employees.

3.3.5 We have not been briefed to examine in detail the broader schema of the Workplace Relations Act, and have not done so. Nevertheless, the Commission may be interested in our preliminary impression regarding possible inconsistency between the Act and any State law regulating the searching or testing of employees. Federal awards cannot deal with subjects like privacy that fall outside the 20 allowable award matters: Workplace Relations Act s 89A. However, there does not seem any reason why certified agreements and, perhaps, workplace agreements could not make provision for the testing or searching of employees, providing these were accepted to be "matters pertaining to the relationship between" employers and employees: Workplace Relations Act ss 170LI and 170VF. In any such case, State provisions dealing with those subjects would be found "operationally" inconsistent with the Commonwealth agreement provisions, which have the force of Commonwealth law. They would then be inoperative in the context of the particular employment relationships governed. [621]

3.3.6 There is unlikely to be any potential for broader inconsistency. Ultimately, the ability of employers to compel employee participation in tests, or to conduct bodily or property searches, will turn on the employee's agreement. The general law dictates that employees would need to consent to any such procedures, though that consent may be made a condition of employment. The evident policy of the Workplace Relations Act, at least since the 1996 reforms, has been to increase opportunities for States and Territories to enter the field of workplace relations regulation. The scaling back of federal awards to 20 allowable award matters has allowed State awards and laws a more wide-ranging operation in the field. The Workplace Relations Act and Regulations do not seem on their terms to address matters of workplace privacy. Nor is there any compelling basis for inferring a Commonwealth intention to preclude State and Territory regulation of those matters.

621 Awards, etc, are acknowledged to have the status of Commonwealth "law" for purposes of s 109 inconsistency analysis, though the precise means by which this result is achieved is not settled: *Ex parte McLean* (1930) 43 CLR 472 at 484 per Dixon J; *Metal Trades Industry Association v Amalgamated Metal Workers' and Shipwrights' Union* (1983) 152 CLR 632.

Accordingly, other than in the operational inconsistency sense explained at 3.3.5 above, the Workplace Relations Act is unlikely to present a problem to a State wishing to regulate the testing and searching practices of employers.

3.3.7 There would not likely be any general inconsistency between the Privacy Act and State laws dealing with the testing and searching of employees. The Privacy Act is clearly intended to regulate only "information privacy". It leaves to the general law the regulation of all other privacy issues, such as those concerning a person's body and property, and so does not purport to cover a relevant "field".[622] There is, however, some small potential for "operational inconsistency". The Privacy Act provides that "an act or practice of an organisation is an interference with the privacy of an individual" where it breaches either a National Privacy Principle or an "approved privacy code" to which the organisation has agreed to bind itself: s 13A(1)(a) and (b). The National Privacy Principles do not contemplate situations of testing or searching, other than if engaged in specifically "for inclusion in a record" (NPP 1.1) which would then enliven the employee records exception in any case. On the other hand, an approved privacy code could, perhaps, include principles going beyond the information privacy context and contemplating other privacy issues, like testing or searching.

3.3.8 Even so, the statutory backing given to approved privacy codes probably stops at the point where a code departs from matters contemplated by the Privacy Act – that is, matters of information privacy. Statutory powers and discretions, like those governing approval of and determinations under approved privacy codes (ss 18BB and 51), are limited by reference to the nature and scope of the empowering legislation: *Morton v Union Steamship Co of New Zealand Ltd* (1951) 83 CLR 402 at 410; *Project Blue Sky Inc v Australian Broadcasting Authority* [1998] HCA 28 at [34] per Brennan CJ. Even where the Privacy Commissioner purported to "approve" particular provisions of a privacy code dealing with testing and searching, this would probably not give those provisions the force of Commonwealth law. Without the force of law, such voluntary undertakings could not generate an inconsistency.

## 3.4 Whether the *Telecommunications (Interception) Act 1979* (Cth) "covers the field" with respect to "monitoring"?

*The Telecommunications (Interception) Act 1979 (Cth)*

3.4.1 The *Telecommunications (Interception) Act 1979* (Cth) ('the Interception Act') was enacted to replace the *Telephonic Communications (Interception) Act*

622 Section 16B of the Privacy Act makes clear that the private sector is only regulated in so far as information is collected "for inclusion in a record".

1960 ('the Telephonic Act'). The long title of the Act describes the legislation as 'An Act to prohibit the interception of telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.' The matters motivating the enactment of the Interception Act included security matters and the detection of narcotic offences (see Second Reading Speech, Telecommunications (Interception) Bill, House of Representatives, 23 August 1979, p.560). However, the Interception Act must be interpreted by reference to its provisions, and it is clear from the provisions of Interception Act that its scope is not defined by reference to particular purposes, and should not be so limited by reference to examples given during the Minister's second reading speech.

3.4.2 In general terms, the scheme of the Interception Act is to prohibit certain activities, and then provide detailed exceptions to those prohibitions. The scope and operation of the Act is marked out by the prohibition provisions, particularly s.7.

*(i) Interception of communications passing over a telecommunications system*

3.4.3 Section 7(1) of the Interception Act provides that a person shall not *intercept*; authorize, suffer or permit another person to intercept; or do any act or thing that will enable him or her or another person to intercept; a *communication passing over* a *telecommunications system*. Central to the operation of the prohibition in s.7(1) are the concepts of 'interception', 'communication', 'passing over' and 'telecommunications system'. Those expressions are further defined in the Act.

3.4.4 Section 6 expands on the concept of 'interception': 'interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'. The Act excludes certain acts from the definition of 'interception': see for example s.6(2) (persons lawfully on the premises) and s.6(2B) (communications to emergency services numbers).

3.4.5 'Telecommunications system' is defined in s.5(1) to mean:

(a) a telecommunications network that is within Australia; or

(b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia;

and includes equipment, a line or other facility that is connected to such a network and is within Australia.

'Telecommunications network' is then defined in s.5(1) to mean 'a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or

series of systems, for carrying communications solely by means of radio communication'. 'Carry' includes transmit, switch and receive (s.5(2)).

'Communication' is defined in s.5(1) to include a 'conversation and a message', in whole or part, whether in the form of: speech, music or other sounds; data; text; visual images; signals; or in any other form or in any combination of forms. 'Passing over' is defined in s.5(1) to include 'being carried'.

3.4.6 The offence created by s.7(1) is not absolute: it is subject to a number of detailed and wide-ranging exceptions. For example, interception of communication or other acts or things that might otherwise have been a breach s.7(1), are exempted from the prohibition in specified circumstances if the prohibited act or thing is done by an employee of a carrier or other person engaged in installation and like acts (s.7(2)(a) and (aa)), or where the interception is by a person installing, connecting or maintaining equipment used for interception pursuant to a warrant (s.s.(2)(ab)). Also exempt are interceptions associated with activities of ASIO officers in detecting listening devices (s.7(2)(ac); see definition of 'listening devices' in s.22 of the *Australian Security Intelligence Organisation Act 1979* (Cth)); interceptions under warrant (s.7(2)(b)); and interceptions by employees of a carrier pursuant to an emergency request (ss.7(2)(c) and 30). Further exemptions operate in relation to urgent acts done by officers of the Australian Federal Police or State Police Forces, without a warrant under Part VI, in certain circumstances and if certain conditions are satisfied (s.7(4) and (5)).

3.4.7 The circumstances in, and the purposes for, which a warrant can be issued are detailed in Parts III and VI. The provisions of Part III authorise the Attorney-General (and, in emergency situations, the Director-General of Security) to issue warrants to authorised ASIO officers, authorising the interception of communications made to or from a telecommunications service (and related activities) in circumstances relating to security or foreign intelligence, or the interception of foreign communications in certain circumstances. The provisions of Part VI regulate the issuing of warrants, by eligible Judges (of a court created by Parliament) or nominated AAT members, to agencies: Commonwealth agencies (the Australian Federal Police and the Australian Crime Authority) and State agencies declared under s.34. These warrants authorise interceptions of communications made to or from a communications service in connection with the investigation of certain offences. The offences include, but are not limited to, murder, kidnapping, narcotics and terrorism offences. The Police Force of Victoria was declared to be an agency for the purposes of Part VI (the Minister having been satisfied that the *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) made satisfactory provision for the conditions set out in s.35 of the Interception Act). Therefore, this State Act serves the purpose of satisfying the conditions under s.35 for the Police

Force of Victoria to be declared a State agency for the purposes of the Interception Act.

*(ii) Dealing with intercepted information*

3.4.8 The second prohibition relates to the use of intercepted information. Section 63 provides:

Subject to this Part, a person shall not, after the commencement of this Part:

(a) communicate to another person, make use of, or make a record of; or

(b) give in evidence in a proceeding;

lawfully obtained information or information obtained by intercepting a communication in contravention of subsection 7(1).

'Proceeding' is defined in s.5(1) to include various state proceedings. A reference to the expression 'lawfully obtained information 'is a reference to 'information obtained (whether before or after the commencement of this section) by intercepting, otherwise than in contravention of subsection 7(1), a communication passing over a telecommunications system' (s.6E(1)). Additionally, s.63(2) prohibits a person from communicating, making use of, making a record of, or giving in evidence in a proceeding, certain warrant related information.

3.4.9 Part VII then sets out a number of exceptions to those prohibitions. For example, certain information obtained by an interception prior to the commencement of Part VII can be communicated, used or recorded for a purpose connected with existing proceedings, or given in evidence in such proceedings (and certain associated uses) (ss.63A, 73); various carrier employee related communications and uses of certain information (ss.63B, 72 and 73); certain communications and uses in connection with ASIO's functions (ss.64, 65, 72); certain communications to agencies or for a prescribed purpose in relation to an agency or Commonwealth Royal Commission (and certain associated uses) (ss.65A, 66, 67, 72, 73); certain communications by an agency to other agencies, the Director-General of Security or Commonwealth Royal Commissions (and certain associated uses) (ss.68, 72); and certain communications between members of police forces (s.70); certain communications and uses in relation to suspected offences against ss.7(1) and 63 of the Interception Act (and associated uses) (ss.71, 72, 73). Additionally, ss.74-78 set out the circumstances in which information obtained by intercepted communications (passing over a telecommunications system), or warrant related information, can be given in various proceedings. Section 77 generally prohibits the giving of evidence in proceedings, except where expressly permitted by the Act.

3.4.10 Parts VIII and IX of the Interception Act regulate in great detail the keeping of records by the AFP and the Australian Crime Commission, and the inspection of those records by the Ombudsman. The Parts also require the reporting of certain information to the relevant Minister, and the reporting by the Minister of certain information to Parliament. Part X creates offences for contravention of ss.7(1) and 63, and other offences relating to non-compliance with certain other provisions of the Interception Act. Part XA creates civil remedies in relation to contraventions of ss.7(1) and 63. Significantly, s.107D provides that Part XA 'is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Part'.

3.4.11 There is no suggestion that the Interception Act is invalid (see *Grollo v Commissioner of Australian Federal Police* (1995) 184 CLR 348; *Love v Attorney-General (NSW)* (1990) 169 CLR 307; *Hilton v Wells* (1985) 157 CLR 57; *John Fairfax Publications Pty Ltd v Doe* (1995) 37 NSWLR 81; *Kizon v Palmer* (1997) 72 FCR 409).

3.4.12 The Telecommunications Interception and other Legislation Amendment Bill 2003 does not affect the scope of the prohibitions in ss.7(1) or 63. The purpose of the amendment is to confer appropriate law enforcement powers on new Western Australian agencies and to expand the offences in relation to which warrants may be issued.

*The Surveillance Devices Act 1999 (Vic)*

3.4.13 The purposes of the *Surveillance Devices Act 1999* (Vic) ('the Surveillance Devices Act') are clearly identified in s.1 of the Act: to regulate the installation, use and maintenance of surveillance devices; to restrict the communication and publication of records of private conversations and activities obtained through the use of surveillance devices; to establish procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation and use of surveillance devices; to create offences relating to the improper installation or use of surveillance devices; to impose requirements for the secure storage and destruction of records obtained by law enforcement officers through the use of surveillance devices and to repeal the *Listening Devices Act 1969* (Vic).

3.4.14 It is immediately apparent from these purposes that the scope and operation of the Surveillance Devices Act overlaps, but is not coextensive with, the Interception Act. This position is confirmed when one views the substantive provisions of the Surveillance Devices Act. Part 2 of the Act regulates the installation, use and maintenance of surveillance devices. Subsection 6(1) provides that 'a person must not knowingly install, use or maintain a listening device to overhear, record, monitor or listen to a private conversation to which the person is not a party, without the express or implied consent of each party to the conversation'. Exceptions from the prohibition are set out

in s.6(2): the installation, use or maintenance of a listening device, either in accordance with a warrant or an emergency authorisation; or in accordance with a law of the Commonwealth.

3.4.15 'Listening device' is defined in s.3(1) to mean 'any device capable of being used to overhear, record, monitor or listen to a private conversation or words spoken to or by any person in private conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear'. 'Warrant' is defined in s.3(1) to mean (other than in ss.33, 34 and 35) a warrant issued under Division 1 of Part 4 of the Surveillance Devices Act. 'Emergency authorisation' means an emergency authorisation given under Division 3 of Part 4 of the Surveillance Devices Act. Similar prohibitions are provided for in relation to the installation, use or maintenance of optical surveillance devices (s.7); tracking devices (s.8); and data surveillance devices (s.9). The exceptions to these other prohibitions mirror the exceptions to s.6(1) – except that a further exception is provided for in the case of s.7 (reasonable installation, use or maintenance by a law enforcement officer).

3.4.16 The authorisation of warrants is dealt with under Part 4 of the Surveillance Devices Act. The Supreme Court of Victoria (all warrants) and the Magistrates' Court of Victoria (some warrants) may issue warrants under the Surveillance Devices Act. Warrants for the installation, use and maintenance of surveillance devices may be issued in relation to the commission of an offence against a Commonwealth, State or Territory law (s.15(1)). The circumstances to be taken into account by a court in determining whether a warrant should be issued are set out in s.17(2), (4). Applications may also be made for the assistance of another person for the effective execution of a warrant (ss.21, 22). Sections 25-30 of the Surveillance Devices Act deal with applications for emergency authorisation for the use of a surveillance device in certain circumstances and in relation to certain offences.

3.4.17 Section 11(1) of the Surveillance Devices Act prohibits a person from knowingly communicating or publishing a record or report of a private conversation or private activity that has been made as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device. Exceptions for various communication or publication are contained in s.11(2): those made with the express or implied consent of each party to the private conversation or private activity; those that are no more than is reasonably necessary in the public interest, or for the protection of the lawful interests of the person making it; those made in the course of legal proceedings or disciplinary proceedings; those made by a law enforcement officer in certain circumstances; certain communications made to police officers; and communications and publications authorised by a law of the Commonwealth relating to the security of the Commonwealth. A similar

prohibition to that in s.11(1) applies to the communication or publication of information obtained from the use of a data surveillance device (s12(1)). The exceptions to the prohibition in s.12(1) are contained in s.12(2) and are similar to the exceptions contained in s.11(2).

3.4.18 Part 6 sets out various record keeping and reporting requirements.

*Direct Inconsistency*

3.4.19 A number of comments may be made about the potential for direct inconsistency between the provisions of the Interception Act and the Surveillance Devices Act. Because of the conclusion reached below that the Interception Act covers the field exclusively, it is unnecessary to give a detailed account of all the direct inconsistencies that might arise. However, the following comments may be made as a guide on those questions.

3.4.20 First, there is clear potential for overlap between some of the activities prohibited by ss.6-9 and the activities prohibited by s.7(1) of the Interception Act. However, clearly, the prohibitions in ss.6-9 of the Surveillance Devices Act are not limited to the interception of communication passing over a telecommunications system (ie, the activity caught by the Interception Act). Secondly, the Surveillance Devices Act, to some extent, seeks to avoid a direct inconsistency from arising by excepting from the prohibitions the installation, use or maintenance of the relevant device 'in accordance with a law of the Commonwealth'. Thus, the interception of a communication passing over a telecommunications system pursuant to a warrant issued under the Interception Act (or other exception under that Act) would not constitute a contravention of the relevant prohibition in the Surveillance Devices Act (see, for example, *Love v Attorney-General (NSW)* (1989) 169 CLR 307, 318).[623]

3.4.21 Thirdly, a warrant under the Surveillance Devices Act is an allowable departure from the prohibition under that Act. It does not constitute a statutory authorisation to engage in the activity contrary to the Commonwealth prohibition in s.7(1). Thus, no direct inconsistency would arise (see, for example, *Love v Attorney-General (NSW)* (1989) 169 CLR 307, 317). If the interception was also prohibited by the Interception Act, a warrant would have to be obtained under that Act to avoid the prohibition in s.7(1).

3.4.22 However, the potential for operational inconsistency remains. There may be circumstances where the Interception Act operates to authorise certain

623 Note also that this would avoid an inconsistency with the listening device provisions contained in the *Customs Act 1901* (Cth); the *Australian Federal Police Act 1979* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth).

activities that would be prohibited by the Surveillance Devices Act (see for example *Miller v Miller* (1978) 141 CLR 269 below). In those circumstances there is potential for direct contradiction between the Interception Act and the Surveillance Devices Act. Further, in circumstances where the same activity would constitute a contravention of both provisions, the penalties for contravention are potentially different, thus giving rise to a direct inconsistency.

3.4.23 Similar comments may be made in relation to the interaction between s.63 of the Interception Act and s.11(1) of the Surveillance Devices Act. For example, s.77 of the Interception Act may prohibit the use of information obtained in breach of the Interception Act, in a way which would otherwise be permitted by s.11(1) of the Surveillance Devices Act. Further, as the brief highlights, the record keeping provisions of the respective Acts contain different standards and, thus, there is the potential for direct inconsistency.

*Indirect inconsistency - scope and operation of the Interception Act (ie, the field of operation)*

3.4.24 It is clear that the scope and operation of the Interception Act are defined by reference to the activity that is the subject of the prohibition in s.7(1). The Act regulates the interception of communications passing over a telecommunications system. The remainder of the Act operates by reference to that activity. The various exceptions to s.7(1) obviously are directly referable to that activity. Additionally, the operation of the prohibition in s.63 (including the exceptions to it) is confined to the communication and various uses of information obtained from interception of communications passing over a telecommunications system, or the communication or other use of warrant related information.[624] Furthermore, other provisions of the Act (eg, record keeping and reporting) operate by reference to that activity or matters following from that activity.

3.4.25 Therefore, the scope and operation of the Act (ie, the field of operation), albeit comprehensive and detailed, is limited, and defined by reference to that activity. The question then is whether the Commonwealth Parliament has expressed an intention to cover that field exclusively.

*Does the Interception Act cover the field?*

3.4.26 There is strong authority for the view that the Interception Act exclusively covers the field of the interception of communications passing over a telecommunications system. As indicated, the Interception Act was enacted to replace the Telephonic Act. In *Miller v Miller* (1978) 141 CLR 269, the

624 That is, information that arises only in consequence of a warrant for the interception of communications passing over a telecommunications system.

High Court held that the Telephonic Act covered the field in relation to telephonic interception, to the exclusion of the *Listening Devices Act 1969* (NSW). The case concerned an act (listening to a telephone conversation on an extension within the same house without permission) that fell within the equivalent Commonwealth provision to the current s.6(2) of the Interception Act. By operation of the equivalent provision to s.6(2), the act of listening in those circumstances was excluded from the definition of 'interception' in the equivalent provision to the current s.6(1) of the Interception Act. The question for the Court was whether the *Listening Devices Act 1969* (NSW) could regulate the act of listening in the circumstances, because that act had been excluded from the definition of 'interception' in the Commonwealth Act. Section 4(1) of the NSW Act prohibited the use of listening devices to hear, record or listen to a private conversation, and s.7(1) prohibited the use of information obtained in breach of s.4(1) in civil or criminal proceedings (subject to exceptions). The High Court held that that the Commonwealth Act evinced an intention to cover the field, including the acts excluded from the definition of 'interception'.

3.4.27 Chief Justice Barwick (with whom Gibbs, Stephen and Aickin JJ agreed; Jacobs J agreeing on the relevant point) considered that the Telephonic Act 'quite clearly intend[ed] that it should be the sole law about telephonic interception and that by reason of its provisions, listening to a telephonic message by means of the telephone extension within premises to which a telephone service is connected by a person lawfully on those premises should be lawful' (at 276). Justice Gibbs added that the Telephonic Act was 'intended to express completely the law governing the interception of communications passing over the telephone system' (at 277). Justice Jacobs made similar comments: 'So far as the prohibitions do not extend there should in my opinion be implied a legislative intention that the use of the telephone system was otherwise permitted, that is to say, an implied intention to cover the whole subject matter of listening to or recording communications over the telephone system without the knowledge of the person making the communication. I am also of the opinion that the Commonwealth Act discloses an implied intention to permit the divulging or communicating of any information obtained by acts which do not amount to an interception' (at 278).

3.4.28 The Court further held that there was a direct inconsistency as the Commonwealth had impliedly made the relevant act lawful, whereas the State legislation had sought to make the relevant Act unlawful. However, the Court made it clear that the State legislation was not wholly invalid (Barwick CJ at 276; Gibbs J at 277; Jacobs J 278). It continued to operate outside the field exclusively covered by the Commonwealth Act. Neither covering of the field nor direct inconsistency would operate beyond the field covered by the Commonwealth Act.

3.4.29 Similar views have been expressed in relation to the operation of the Interception Act. In *R v Curran and Torney* [1983] 2 VR 133, McGarvie J concluded that the Interception Act 'shows a legislative intention that it be the exclusive law upon telephonic interception both for what it forbids and what it allows. Accordingly, the [*Listening Devices Act 1969* (Vic)] did not apply' to the relevant conduct (at 153).

3.4.30 In *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222, Lee J considered that there was nothing in the Interception Act 'to indicate any departure from the intention found to have been present in the [Telephonic Act]' (at 230). Thus, his Honour held that the Interception Act covered the field of telecommunications interception, and the *Listening Devices Act 1969* (NSW) and, its successor, the *Listening Devices Act 1984* (NSW) could have no operation on the interception of such communications. Justice Lee's construction of the legislation was upheld by the NSW Court of Criminal Appeal in *R v Edelsten* (1990) 21 NSWLR 542 (although no question of s.109 was discussed). In refusing leave to appeal to the High Court, Gibbs J observed that *Miller v Miller* appeared to govern the question of inconsistency (see *Edelsten,* at 230 (Lee J)).

3.4.31 A similar view was expressed by Butler J in *In Marriage of Parker and Williams* (1993) 117 FLR 1. Referring to *Miller v Miller,* his Honour said, 'it is not open to doubt that the [Interception Act] covers the field of interception of telecommunications, just as the [Telephonic Act] did before the [Interception Act]' (at 7-8). Thus, the provisions of the *Listening Devices Act 1991* (Tas) could not enter that field. That position has been accepted in other cases: see *Byrne v Byrne* (2002) 172 FLR 81, at [29]; *Violi v Berrivale Orchards* (2000) 173 ALR 518, 520; *R v McHardie and Danielson* [1983] 2 NSWLR 733, 746).

3.4.32 None of the judgments engage in detailed analysis to establish the proposition that the Interception Act exclusively covers the relevant field. Since that intention is not stated explicitly in the Interception Act, it must arise by implication from the terms of the Act. In our view, an analysis of the provisions of the Interception Act supports the proposition established by the cases. First, the field covered is a narrow one: 'the interception of communications passing over a telecommunications system.' Given that limited focus, it is strongly arguable that the Commonwealth Parliament intended to have sole control of that area, and that *any* intrusion by the States would frustrate the operation of the Interception Act.

3.4.33 Secondly, the Interception Act sets up a detailed legislate scheme to prohibit certain activity, and then relaxes those prohibitions for certain purposes or in certain circumstances. The detailed nature of the provisions suggests that the Interception Act contains a legislative judgment about the competing public interests associated with the imposition of the prohibitions and their

relaxation, and that there would be no room for State legislation to operate side-by-side with the Interception Act, even if it were to operate in a way that did not give rise to a direct inconsistency.

3.4.34 Thirdly, the detailed scheme of exceptions is not limited to Commonwealth officers, proceedings and offences. For example, the Act allows certain State law enforcement agencies (including the Police Force of Victoria) to apply for warrants when investigating certain state offences. The Act also deals with the circumstances in which intercepted communications can be received in state proceedings. In determining the circumstances that would justify a relaxation of the prohibitions in the Interception Act, it is strongly arguable that the Commonwealth Parliament has made a judgment about those state officers who may be permitted to depart from the prohibitions, the types of state offences that would warrant such a departure, and the way in which intercepted communication may be dealt with in state proceedings. Arguably, such a legislative scheme leaves no room for state regulation.

3.4.35 Fourthly, in the context of creating civil remedies in relation to breaches of the Act (Part XA), s.107D provides that Part XA 'is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Part.' The fact that the Parliament has specifically provided for the concurrent operation of State laws in relation to one aspect of the operation of the Interception Act, is textual support for the proposition that, in relation to other aspects, the Act did not contemplate concurrent operation.

### 3.5 Whether the *Surveillance Devices Act 1999* (Vic) is capable of regulating "monitoring" of private sector employee communications or is invalid pursuant to s 109 of the Constitution because it is inconsistent with the *Telecommunications (Interception) Act 1979* (Cth)?

3.5.1 The Interception Act exclusively covers the field of 'interceptions of communications passing over a telecommunications system'. Following the decision in *Miller v Miller,* that field would extend to acts that would otherwise constitute 'interceptions' for the purposes of the Act, but for their exclusion from the meaning of 'interception' by s.6(2) of the Act. State legislation, including the *Surveillance Devices Act 1999* (Vic) cannot operate in that field in any way. However, the field covered by the Interception Act would not be co-extensive with the listening, recording or monitoring of private sector employee communications. Only to the extent that listening, recording or monitoring involves the interception of communications passing over a telecommunications system would those activities be within the field covered by the Interception Act. To the extent that listening, recording or monitoring does not involve the interception of communications passing over a telecommunications system, State legislation could validly operate in relation

to those activities. Whether or not listening, recording or monitoring would involve the interception of communications passing over a telecommunications system would depend upon the type of listening, recording or monitoring activity undertaken.

3.5.2 It then becomes important to determine when an activity will be an 'interception of a communication passing over a telecommunications system'. Since this question is not directly relevant to the constitutional questions that have been asked, we will not deal with it in any detail. However, some brief observations may be made. There has been some disagreement about the purposes sought to be achieved by the Interception Act and the circumstances in which there will be an 'interception of a communication passing over a telecommunications system'. Undoubtedly, the numerous amendments made to the Act have contributed to this uncertainty. In relation to the purpose of the Act, Butler J in *Parker* saw the purpose as maintaining 'the integrity of telecommunications' rather than being 'directly concerned with the protection of privacy or the right to privacy' (at 10). A concern for the integrity of the system also seemed to be a matter referred to by Barwick CJ in *Miller*, in the context of the Telephonic Act (at 276). See also *R v Migliorini* [1981] Tas R 80, 88.

3.5.3 However, the predominant view appears to be that the Interception Act is concerned to protect, at least in part, the privacy of communications passing between users of the system (*Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222, 229; *R v Edelsten* (1990) 21 NSWLR 542, 549; *T v Medical Board (SA)* (1992) 58 SASR 382, 398; *Green v The Queen* (1995) 124 FLR 423, 431-2; *Taciak v Commissioner of Australian Federal Police* (1995) 59 FCR 285, 297-8; *Kizon v Palmer* (1997) 72 FCR 409, 442; *John Fairfax Publications Pty Ltd v* Doe (1995) 37 NSWLR 81, 97; *R v Evans* (1999) 152 FLR 352, 363; *Byrne v Byrne* (2002) 172 FLR 81, [29]).

3.5.4 In relation to what would constitute an 'interception of a communication passing over a telecommunications system', it appears that the predominant view is that the taping of a telephone conversation before it enters into the mouthpiece, or after it leaves the earpiece (*R v Migliorini* [1981] Tas R 80, 88; *In the Marriage of Parker and Williams* (1993) 117 FLR 1, 11; *R v Giaccio* (1997) 68 SASR 484, 491; *Violi v Berrivale Orchards Ltd* (2000) 173 ALR 518; *R v Luzlim Bandulla* [2001] VSCA 202, [12]; but cf, *R v Curran and Torney* [1983] 2 VR 133, 153; *T v Medical Board* (SA) (1992) 58 SASR 382, 421 (Olsson J)); or the taping by one of the parties to the telephone conversation (*T v Medical Board* (SA) (1992) 58 SASR 382, 398-9 (Matheson J); *Green v The Queen* (1996) 124 FLR 423; *R v Evans* (1999) 152 FLR 352, 364-5; *Byrne v Byrne* (2002) 172 FLR 81, [33] ), will not be covered. Relevantly for present purposes, in *R v Evans,* McDonald J held that the recording by an employer of employees' telephone conversations,

whilst they were acting in the course of their employment, did not constitute 'interception' for the purposes of the Interception Act.

3.5.5 The briefing paper suggests that there may be some doubt as to whether the monitoring of email would be an 'interception of a communication passing over a telecommunications system'. A resolution of this issue would require more detailed technical information than has been provided. However, we can offer the following observations. First, the recent discussion paper by the Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers assumes that email, internet usage and other computer transmissions are regulated by the Interception Act (see 'Cross-Border Investigative Powers for Law Enforcement', February 2003, p.215). Secondly, the words 'interception of a communication passing over a telecommunications system' are capable of a flexible interpretation. For example, in *Edelsten,* Lee J held (and the NSW Court of Criminal Appeal agreed) that a communication using a car telephone picked up by a scanner was a 'communication passing over a telecommunications system' that was 'intercepted' for the purposes of the Interception Act.

3.5.6 We would be happy to provide more detailed advice if required on what would constitute an 'interception of a communication passing over a telecommunications system'.

**3.6 Guidance on the constitutional implications of the various models by which workplace privacy might be regulated at the State level.**

3.6.1 The briefing paper has not provided any details about the various models that might be contemplated to regulate workplace privacy. Therefore, the following comments are necessarily general in nature. We would be happy to provide more detailed advice on particular models that might be formulated.

3.6.2 It is apparent from the discussion above that, subject to further regulation at the Commonwealth level, there is considerable scope for State Parliaments to regulate some aspects of workplace privacy. As a matter of general constitutional principle, State legislative power is plenary: legislation of a State parliament is 'valid if there is any real connexion – even a remote or general connexion – between the subject matter of the legislation and the State' (*Mobil Oil Australia Pty Ltd v Victoria* (2002) 189 ALR 161, [48], quoting from *Pearce v Florenca* (1976) 135 CLR 507, 518 (Gibb J)). Of course, State legislative power is subject to any limitation on that power, whether express or implied, in the Constitution, and is subject to s.109 of the Constitution.

3.6.3 As a general matter, regulation of workplace privacy would fall within State legislative power. In the absence of the details of a specific model for the

regulation of workplace privacy, it is difficult to speculate as to whether a constitutional limitation might be breached. As to s.109, whether an inconsistency arises depends upon the operation of Commonwealth legislation. In the context of the Interception Act, the field exclusively occupied by the Commonwealth and, thus, the potential for state regulation, is clearly marked out by the operation of the Interception Act. Thus, subject to further Commonwealth legislative activity, a State Parliament could regulate outside that field. In relation to the *Privacy Act* and the *Workplace Relations Act*, State legislation that sought clearly to identify a field of operation that could be differentiated from the fields covered by the Commonwealth Acts would have a greater chance of avoiding the operation of s.109. Thus, for example, State legislation that sought to regulate workplace activities, with a focus on protecting privacy not protected by the *Privacy Act*, might be considered to operate side-by-side with both the *Privacy Act* and *Workplace Relations Act.*

3.6.4 Of course, clear statements of purpose will not save the State law in cases of direct inconsistency, or where the Commonwealth in the future, or in other legislation, expresses an intention exclusively to cover part of the field covered by the State legislation. However, clear statements of intention will assist in differentiating a field of activity for the State law.

3.6.5 It is important also to note that the exercise of State legislative power might be limited if it gives rise to a conflict with the laws of another State. The possibility of conflict between State laws has been recognised by the High Court, but a method for resolving that conflict is yet to be established (see *Mobil* (2002) 189 ALR 161, [48]; and *John Pfeiffer Pty Ltd v Rogerson* (2000) 203 CLR 503, [3]). In practical terms, since State Parliaments usually regulate matters within their respective territorial limits, a conflict is unlikely to arise (see Kirby J in *Mobil* (2002) 189 ALR 161, [108]).

3.6.6 Our understanding is that the Commonwealth and States may be considering the possibility of enacting co-operative schemes for the regulation of some aspects of workplace privacy. In considering whether such schemes would be constitutionally permissible, the High Court's decision in *R v Hughes* (2000) 202 CLR 535 would be important. For example, in many co-operative schemes, powers and duties are conferred by both the Commonwealth and State Parliaments on government officers or authorities. The High Court's decision in *Hughes* limits the extent to which State Parliaments can confer those powers and duties on Commonwealth officers and authorities. If state power is lacking, but the Commonwealth and States nevertheless want to pursue the co-operative scheme, the State Parliaments would need to consider referring power to the Commonwealth Parliament pursuant to s.51(xxxvii) of the Constitution. Recent examples of areas in which matters have been referred to the Commonwealth Parliament include the regulation of corporations and anti-terrorism activities. Also, as your briefing paper

notes, Victoria has referred power to the Commonwealth Parliament by virtue of the *Commonwealth Powers (Industrial Relations) Act 1996* (Vic).

3.6.7 These comments are necessarily general, and we would be happy to expand upon them if required.

**Amelia Simpson**
**James Stellios**

**Faculty of Law**
**Australian National University**

29 September 2003

# Appendix 5

## TABLE 1: PRIVACY LAWS RELEVANT TO WORKERS

| Area of Privacy | Relevant Law | Coverage | Limits to Coverage |
|---|---|---|---|
| **Information** | *Privacy Act 1988* (Cth) | Commonwealth public sector and private sector organisations | • Does not cover most small businesses<br>• Does not cover employee records |
| | *Information Privacy Act 2000* (Vic) | Victorian public sector | |
| | *Health Records Act 2001* (Vic) | Health service providers (both Victorian public and private sector) | • Only covers 'health information', but includes health information in employee records |
| **Communications** | *Telecommunications (Interception) Act 1979* (Cth) | Interception of telecommunications | • Does not apply where employee is aware of the monitoring |
| **Surveillance** | *Surveillance Devices Act 1999* (Vic) | The installation, use and maintenance of listening, optical surveillance, tracking and data surveillance devices<br>The publication or communication of material obtained from the use of the devices | • Not available if person consents<br>• Regulation of listening devices only protects private conversations<br>• Regulation of optical surveillance devices only protects private activities<br>• Regulation of listening and optical surveillance devices do not apply where a person who is a party to the activity uses the device<br>• Regulation of data surveillance devices limited to use by law enforcement officer |
| **Territorial,** for example, body or property searches | Criminal law<br>Common law remedies, for example, battery | Apply generally in the community | Not available if person consents |

# Appendix 6

## TABLE 2: WORKPLACE RELATIONS LAW RELEVANT TO WORKER PRIVACY

| Relevant Law | Mechanisms | Remedies | Limits to Privacy Protection |
|---|---|---|---|
| *Workplace Relations Act 1996* (Cth) | Awards | | Privacy not an allowable award matter |
| | Certified Agreements | Dispute resolution procedures in an AWA or certified agreement could be used to resolve privacy disputes | Privacy protection (in both certified agreements and AWAs) limited by bargaining strength of parties |
| | Australian Workplace Agreements | | |
| | Unfair dismissal | Compensation | Only available to limited categories of workers<br>Only available at end of employment relationship |
| | Unlawful termination | Compensation<br>Penalties | |
| | Unfair contracts | Variation or setting aside of contract | Limited to independent contractors |
| Contract of employment | Implied employer duty of trust and confidence | Damages for breach of contract | Limited to employer/ employee relationships<br>Not fully described in Australian law |
| *Occupational Health and Safety Act 1985* (Vic) and *Accident Compensation Act 1985* (Vic) | | Compensation for injuries (physical or mental) suffered in the workplace | Incidental privacy protection (eg protects against victimisation and bullying) |
| *Equal Opportunity Act 1995* (Vic) | | Complaint of discrimination and harassment can be made to the Equal Opportunity Commission | Incidental privacy protection. Can be seen to protect the 'autonomy and dignity' of job applicants and workers (for example, through the prohibition on requesting information that could be used to form the basis of discrimination) |

# Bibliography

American Management Association, *2001 AMA Survey on Workplace Testing: Medical Testing* Summary of Key Findings (New York, 2001)

Anti-Discrimination Board of New South Wales, *C Change: Report of the Enquiry into Hepatitis C Related Discrimination* (2001)

Attorney-General's Department and the Department of Employment and Workplace Relations, *Employee Records Privacy: A Discussion Paper on Information Privacy and Employee Records* (ACT, 2004)

Australian Centre for Industrial Research and Training, *Fitness for Duty—Recent Legal Developments* Working Paper 69 (2001)

Australian Communications Industry Forum, *Industry Guideline: Participant Monitoring of Voice Communications* ACIF G516:2004 (2004)

Australian Law Reform Commission, *Essentially Yours: the Protection of Human Genetic Information in Australia, Volume 2* Report 96 (2003)

Australian Medical Association, *Independent Medical Assessments on Behalf of Parties Other Than the Patient: 1998 as Amended 2002* AMA Position Statement (2002)

Australian Medical Association, *Code of Ethics* (May 2003)

Australian Nursing Council, *Code of Professional Conduct for Nurses in Australia* (2003)

Australian Nursing Council, Australian Nursing Federation and Royal College of Nursing, Australia, *Code of Ethics for Nurses in Australia* (Revised 2002)

Australian Psychological Society, *Comments for Victorian Law Reform Commission's Psychological Testing Technical Consultation Group* (2003)

Australasian Faculty of Occupational Medicine, *Guidelines for Health Assessments for Work* (Royal Australasian College of Physicians, 1998)

ASX Corporate Governance Council, *Principles of Good Corporate Governance and Best Practice Recommendations* (2003)

Baldwin, Robert and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press, 1999)

Black, Julia, 'Managing Discretion' (Paper presented at the 'ALRC Conference, Penalties: Policy, Principles and Practice in Government Regulation, 7 June 2001', Sydney)

Braithwaite, John and Ian Ayres, *Responsive Regulation* (Oxford University Press, 1992)

CNIL, *Cyber-Surveillance in the Workplace: A Report presented by Mr Hubert Bouchet, Delegate Vice-Chairman of the CNIL* (Paris, 2002)

*Code of Behaviour for Psychologists* (1997) Psychologists Registration Board of Victoria <www.psychreg.vic.gov.au> at 31 August 2004

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11*

Craig, John, *Privacy and Employment Law* (Hart Publishing, 1999)

Creighton, Breen and Andrew Stewart, *Labour Law: An Introduction* (3rd ed) (Federation Press, 2000)

Davis, Mark, 'Employment Selection Tests and Indirect Discrimination: The American Experience and Its Lessons for Australia' (1996) 9 *Australian Journal of Labour Law* 187

Delbridge, A, JRL Bernard, D Blair, et al (eds), *The Macquarie Dictionary* (3rd ed) (The Macquarie Library, 1997)

Department of Justice, *New Directions for the Victorian Justice System 2004–2014: Attorney-General's Justice Statement* (Victoria, 2004)

Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (Electronic Privacy Information Center, Washington, 2003)

Equal Opportunity Commission Victoria, *Employer Guidelines: Pre-Employment Medical Testing* (Equal Opportunity Commission Victoria)

Equal Opportunity for Women in the Workplace Agency, *2003 Australian Census of Women Executive Managers* Fact Sheet

Ferguson, Adele, 'Science, Cynicism and the Cult of Personality Testing' *Business Review Weekly* 23 September 1996,

Foord, Kate, *Defining Privacy* Occasional Paper (Victorian Law Reform Commission, 2002)

*France: Works Rules* European Foundation for the Improvement of Living and Working Conditions www.eurofound.eu.int/emire/FRANCE/WORKSRULES-FR.html> at 29 June 2004

Freehill, Hollingdale & Page, *Internet Privacy Survey Report* (2000)

Godfrey, Kelly, 'Contracts of Employment: Renaissance of the Implied Term of Trust and Confidence' (2003) 77 *Australian Law Journal* 764

Grabosky, Peter, 'Regulation by Reward: On the Use of Incentives as Regulatory Instruments' (1995) 17 (3) *Law and Policy* 257

Griffiths, Dave, *Psychometric Testing in Recruitment* Nelson Griffiths <www.nelsongriffiths.com/psychometric.pdf> at 28 April 2004

Holland, Peter and Mark Wickham, 'Drug Testing in the Workplace: Unravelling the Issues' (2002) 18 (1) *Journal of Occupational Health and Safety Australia and New Zealand* 55

Howell, Wayne, 'Lie Detector Boom' *The Herald Sun* (Melbourne) 26 July 2004, 15

'ILO and Pre-Employment Pregnancy Testing' (1999) 106 *Unity News: Weekly News*

International Labour Office, *Workers' Privacy—Part II: Monitoring and Surveillance in the Workplace* 12(1) (Geneva, 1993)

*Management of Alcohol- and Drug-Related Issues in the Workplace* An ILO Code of Practice (Geneva, 1996)

*Technical and Ethical Guidelines for Workers' Health Surveillance* (Geneva, 1998)

Harcourt, Victor, 'The Doctor, the Third Party and the Examinee: Is There a Duty to Inform' (2000) 8 *Torts Law Journal* 221

Hawkins, Keith, *Environment and Enforcement: Regulation and the Social Definition of Pollution* (Clarendon Press, Oxford, 1984)

Heiler, Kathryn, 'Drugs and Alcohol Management and Testing Standards in Australian Workplaces: Avoiding that "Morning-After" Feeling' (Paper presented at the 'Drugs and Alcohol at the Workplace: Testing Issues and After Hours Conduct: Breakfast Briefing, Thursday 5 December 2002', Sydney)

Hicks, R E, 'Psychological Testing in Australia in the 1990's' (1991) *Asia Pacific Human Resource Management* 94

Information and Privacy Commissioner, *Workplace Privacy: A Consultation Paper* (Ontario, 1992)

Information Commissioner, *The Employment Practices Data Protection Code: Part 3: Monitoring at Work* (Cheshire UK)

Jenkinson, Jo, 'The Skill Basis of Psychological Testing' (1991) 4 (1) *Psychological Test Bulletin* 5

Johnson, Graeme, 'The Reference Power in the Australian Constitution' (1973) 9 (1) *Melbourne University Law Review* 42

Johnston, Anna and Myra Cheng, 'Electronic Workplace Surveillance, Part 1: Concerns for Employees and Challenges for Privacy Advocates' (2003) 9 (9) *Privacy Law & Policy Reporter* 161

'Electronic Workplace Surveillance, Part 2: Responses to Electronic Workplace Surveillance—Resistance and Regulation' (2003) 9 (10) *Privacy Law & Policy Reporter* 187

Kendall, Ian, Jo Jenkinson, Molly de Lemos, et al, *Supplement to Guidelines for the Use of Psychological Tests* (The Australian Psychological Society, 1997)

Lane, Frederick, *The Naked Employee: How Technology is Compromising Workplace Privacy* (AMACOM, New York, 2003)

Laufer, Suzie, 'Medico-Legal Conference on Individual Testing and Review, Bond University, June 1991' (1991) 65 *Australian Law Journal* 584

*Levels of Proof Instructions* National College of DUI Defense, Inc <www.ncdd.com/lop-inst.html> at 17 June 2004

Lyons, Paul, 'Mind a Test?—Psychometric Tests and Personnel Selection' (1990) 61 (4) *Charter* 30

McCallum, Ronald, *Employer Controls over Private Life* (University of New South Wales Press, 2000)

Magnusson, R, 'Privacy, Surveillance and Interception in Australia's Changing Telecommunications Environment' (1999) 27 (1) *Federal Law Review*

Maltby, Lewis, *Drug Testing: A Bad Investment* (American Civil Liberties Union, 1999)

Morris, Caroline, 'Drugs, the Law, and Technology: Posing Some Problems in the Workplace' (2002) 20 *New Zealand Universities Law Review* 1

Mrland, J, *Types of Drug-Testing Programmes in the Workplace* (1993) United Nations: Office on Drugs and Crime <www.unodc.org/unodc/fr/bulletin/bulletin_1993-01-01_2_page004.html> at 17 June 2004

Nelson, Diana and Santina Perrone, *Understanding and Controlling Retail Theft* Trends & Issues in Crime and Criminal Justice, No 152 (Australian Institute of Criminology, 2000)

NetAlert and the Australian Broadcasting Authority, *Effectiveness of Internet Filtering Software Products* (2001)

New South Wales Law Reform Commission, *Surveillance: An Interim Report* 98 (2001)

Nolan, Jim, 'Employee Privacy in the Electronic Workplace Pt 2: Drug Testing, Out of Hours Conduct and References' (2000) 7 (7) *Privacy Law and Policy Reporter* 139

Nygh, Peter and Peter Butt (eds), *Butterworths Australian Legal Dictionary* (Butterworths, 1997)

Office of the Data Protection Commissioner, *The Use of Personal Data in Employer/Employee Relationships* Draft Code of Practice (United Kingdom, 2000)

Paterson, Moira, 'Monitoring of Employee Emails and other Electronic Communications' (2002) 21 (1) *University of Tasmania Law Review* 1

Peterson, Moira and Ea Mulligan, 'Disclosing Health Information Breaches of Confidence, Privacy and the Notion of the "Treating Team"' (2003) 10 *Journal of Law and Medicine* 460

Pittard, Marilyn, 'The Dispersing and Transformed Workplace: Labour law and the Effect of Electronic Work' (2003) 16 (1) *Australian Journal of Labour Law* 69

*Postal Workers Reject New Sick Leave Policy* (2003) ABC Online: 9 December 2003 <www.abc.net.au> at 30 March 2004

*Pre and Post Employment Medicals* (2003) Corporate Medical Options <www.corporate-medical.com.au> at 29 April 2004

'Prepare to be Scanned' *The Economist* 6 December 2003, 15

PricewaterhouseCoopers, *Privacy Survey 2000*

Privacy Committee of New South Wales, *Drug Testing in the Workplace* No 64 (1992)

*Invisible Eyes: Report on Video Surveillance in the Workplace* No 67 (1995)

Robinson, Paul, 'Workplace Psych Tests Widen' *The Age* 18 March 2004

Saul, Peter, 'Psychological Testing in the Selection Process' (1980) 6 (2) *Work and People* 19

Schulman, Andrew, 'Computer and Internet Surveillance in the Workplace' (2001) 8 (3) *Privacy Law and Policy Reporter* 49

Sempill, Julian, 'Call Centres: Total Control Made Easy' in *Case Study, Principles of Labour Law*, (1999)

'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labour Law* 111

Shahandeh, Behrouz and Joannah Caborn, 'Ethical Issues in Workplace Drug Testing in Europe' (Paper presented at the 'Seminar on Ethics, Professional Standards and Drug Addiction, 6–7 February 2003', Strasbourg)

Standards Australia/Standards New Zealand, *Procedures for the Collection, Detection and Quantitation of Drugs of Abuse in Urine* AS/NZS 4308:2001 (2001)

Thompson, Clive, 'Dangerous Minds' *Good Weekend: The Age Magazine* 3 April 2003, 20

United Nations, *Universal Declaration of Human Rights* , adopted and proclaimed by General Assembly resolution 217 A (111) of 10 December 1948

*USA: Providing Protection with Legislation* (2004) PersonnelToday <www.personneltoday.com> at 30 March 2004

Van den Broek, Diane, *Surveillance, Privacy and Work Intensification within Call Centres* WorkSite <www.econ.usyd.edu.au/wos/worksite/surveillance.html> at 5 April 2004

Victorian Law Reform Commission, *Workplace Privacy* Issues Paper (2002)

Walker, Robbie and Ballanda Sack, 'Drug and Alcohol Testing' (2003) (12) *OHS Alert* 1

Williams, George, *Labour Law and the Constitution* (Federation Press, 1998)

Willox, Philip, 'Alcohol and Drugs in the Workplace' (1999) 15 (10) *Australian Company Secretary* 444

Winnett, Ashley, *Critically Examine and Assess the Approach of the Australian Industrial Relations Commission to Dismissal of Employees for Breach of Internet and Email Usage Policy* (Unpublished Essay)

# Other VLRC Publications

*Disputes Between Co-owners: Discussion Paper* (June 2001)

*Privacy Law: Options for Reform—Information Paper* (July 2001)

*Sexual Offences: Law and Procedure—Discussion Paper* (September 2001) (Outline also available)

*Annual Report 2000–01* (October 2001)

*Failure to Appear in Court in Response to Bail: Draft Recommendation Paper* (January 2002)

*Disputes Between Co-owners: Report* (March 2002)

*Criminal Liability for Workplace Death and Serious Injury in the Public Sector: Report* (May 2002)

*Failure to Appear in Court in Response to Bail: Report* (June 2002)

*People with Intellectual Disabilities at Risk—A Legal Framework for Compulsory Care: Discussion Paper* (June 2002)

*What Should the Law Say About People with Intellectual Disabilities Who are at Risk of Hurting Themselves or Other People? Discussion Paper in Easy English* (June 2002)

*Defences to Homicide: Issues Paper* (June 2002)

*Who Kills Whom and Why: Looking Beyond Legal Categories* by Associate Professor Jenny Morgan (June 2002)

*Annual Report 2001–02* (October 2002)

*Workplace Privacy: Issues Paper* (October 2002)

*Defining Privacy: Occasional Paper* (October 2002)

*Sexual Offences: Interim Report* (June 2003)

*Defences to Homicide: Options Paper* (September 2003)

*Annual Report 2002-03* (October 2003)

*People with Intellectual Disabilities at Risk: A Legal Framework for Compulsory Care* (November 2003)

*Assisted Reproductive Technology & Adoption: Should the Current Eligibility Criteria in Victoria be Changed? Consultation Paper* (December 2003)

*People with Intellectual Disabilities at Risk: A Legal Framework for Compulsory Care Report in Easy English* (July 2004)

*Sexual Offences: Final Report* (August 2004)

*The Convention on the Rights of the Child: The Rights and Best Interests of Children Conceived Through Assisted Reproduction: Occasional Paper* by John Tobin (September 2004)

*A.R.T., Surrogacy and Legal Parentage: A Comparative Legislative Review: Occasional Paper* by Adjunct Professor John Seymour and Ms Sonia Magri (September 2004)

*Outcomes of Children Born of A.R.T. in a Diverse Range of Families* By Dr Ruth McNair (September 2004)