

Victorian
Law Reform
Commission

Workplace Privacy
Final Report

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

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 report reflects the law as at September 2005.

© October 2005 Victorian Law Reform Commission. This work is protected by the laws of copyright. Except for any uses permitted under the *Copyright Act 1968* (Cth) or equivalent overseas legislation, no part of this work may be reproduced, in any manner or in any medium, without the written permission of the publisher. All rights reserved.

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 : final report.

Bibliography.

ISBN 0 9757006 4 2

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

344.945012596

Ordered to be printed

Victorian Government Printer

No 159 Session 2003–05

Contents

| | |
|---|-----------|
| CONTRIBUTORS | VII |
| TERMS OF REFERENCE | VIII |
| ABBREVIATIONS | IX |
| EXECUTIVE SUMMARY | XI |
| RECOMMENDATIONS | XX |
| CHAPTER 1: INTRODUCTION | 1 |
| Purpose of this Report | 2 |
| Our Approach to the Reference | 2 |
| Who is a Worker? | 10 |
| Our Process | 11 |
| Structure of the Report | 13 |
| CHAPTER 2: THE CASE FOR REFORM | 15 |
| Introduction | 15 |
| Protection of Privacy as a Human Right | 15 |
| Advances in Technology | 17 |
| Lack of Certainty | 18 |
| Gaps in Legal Protection | 20 |
| Consent and Invasions of Workplace Privacy | 23 |
| Other Jurisdictions | 24 |
| Conclusion | 27 |
| Feedback on the Options | 28 |
| Hybrid Model | 34 |
| CHAPTER 3: BALANCING EMPLOYER AND WORKER INTERESTS | 35 |
| Introduction | 35 |
| Regulatory Framework | 36 |
| Work-related and Non-work-related Activities | 39 |

| | |
|---|------------|
| Balancing Employers' and Workers' Interests at Work | 45 |
| Privacy Protection for Workers when not Working | 69 |
| Other Practices Requiring Authorisation | 74 |
| Prohibited Practices | 84 |
| Other Legislation | 86 |
| CHAPTER 4: PROMOTING COMPLIANCE | 89 |
| Introduction | 89 |
| Statutory Office to Oversee Legislation | 90 |
| Regulator Functions | 94 |
| Promoting Compliance through Education | 95 |
| Resolving Complaints | 96 |
| Why a Systemic Approach is Necessary | 97 |
| Going Beyond the Terms of a Particular Complaint | 99 |
| Undertaking an Inquiry | 99 |
| Advising Government on Workplace Privacy | 101 |
| Individual Complaints Resolution Process | 103 |
| Protecting Workers Against Victimisation | 112 |
| Ensuring Compliance—Sanctions Pyramid | 114 |
| VCAT Hearing and Review | 119 |
| Supreme Court Appeal | 121 |
| APPENDIX 1: ROUNDTABLES | 124 |
| APPENDIX 2: CONSULTATIONS | 126 |
| APPENDIX 3: OPTIONS PAPER SUBMISSIONS | 130 |
| APPENDIX 4: ISSUES PAPER SUBMISSIONS | 132 |
| APPENDIX 5: DRAFT BILL | 135 |
| BIBLIOGRAPHY | 197 |

Preface

The publication of this Final Report is the result of an extensive investigation into the protection of people's privacy while they are at work. It is the first stage of a two-part reference into privacy—the second stage will focus on surveillance in public places.

The report contains 65 recommendations which seek to introduce a regulatory scheme which will provide a transparent framework for workplace privacy protection in Victoria. We have recommended the government introduce a Workplace Privacy Act and establish a statutory office to educate employers and workers and oversee the operation of the Act.

We have recognised the different expectations of privacy protection that many people have when in public or private places. Our recommendations have extended this notion to differentiate between privacy of work-related and non-work-related activities to cover the modern concepts of work and acknowledge its intrusion into what were once considered private spheres.

We have already published an Issues Paper and an Options Paper which identified and discussed the gaps which existed in privacy protection for Victorian workers. Both papers attracted many considered and influential submissions and provided fodder for our invaluable expert roundtables.

Production of this report was a team effort by the commission's staff but special mention must be made of the authors Priya SaratChandran and Susan Coleman. Their professionalism and detailed knowledge of the subject has already been praised by participants in the process, and has resulted in the timely development of the report's recommendations. Members of the commission's Workplace Privacy Division, Professor Sam Ricketson and Australian Industrial Relations Commission Vice-President, the Honourable Iain Ross, also worked hard to ensure the workability of the recommendations in this report, which appears just one year after publication of the Options Paper.

Other staff at the commission who helped with the report include Alison Hetherington who edited, Trish Luker who proofread and Julie Bransden who prepared the bibliography. Simone Marrocco checked footnotes and Kathy

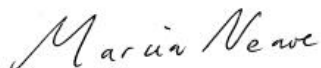
Karlevski prepared the report for publication and distribution. Our CEO, Padma Raman, provided valuable advice throughout various stages of the report's writing.

The law firms Freehills and Deacons won the tender to provide the authors for this report, and my thanks goes to both of them for their flexibility in allowing the authors time to complete the project.

A number of other people have provided us with important direction and advice as we have developed our recommendations. First, the union and employer representatives who made submissions to our Options Paper and participated in our roundtables. Their feedback on the practicalities of suggested options was essential for the development of our recommendations. We have been impressed by their cooperative approach and hope they will appreciate our attempts to balance their competing interests.

We are grateful to all our consultants who generously offered us their time and expertise, but I would like to make particular mention of Mr Matthew Carroll, CEO Equal Opportunity Commission of Victoria; Mr Paul Chadwick, Victorian Privacy Commissioner; Dr Breen Creighton, Corrs Chambers Westgarth lawyers; Ms Penny Dedes, Senior Legal Officer, Equal Opportunity Commission of Victoria; Professor Arie Freiberg, Dean, Monash University Law School; Associate Professor Beth Gaze, Monash University Law School; Mr David Lindsay, Monash University Law School; the Hon the President Justice Chris Maxwell, Victorian Supreme Court of Appeal; Mr Mike Thompson, Director, Linus; and Ms Beth Wilson, Victorian Health Services Commissioner.

Finally, my boundless gratitude goes to the Office of the Chief Parliamentary Counsel for finding the time in its already crowded schedule to prepare the draft Bill which appears at the end of this report. Ms Diana Fagan, Mr Eamonn Moran QC and Ms Gemma Varley all worked on the drafts for the Bill, which has been extremely useful in helping us to develop the regulatory scheme we outline in the following pages.



Marcia Neave
Chairperson

Contributors

Authors

Priya SaratChandran
Susan Coleman

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
Her Honour Judge Felicity Hampel*
Professor Sam Ricketson*
The Honourable Iain Ross AO*
The Honourable Justice Tim Smith

Chief Executive Officer

Padma Raman

Operations Manager

Kathy Karlevski

Policy and Research Team Leaders

Angela Langan
Mary Polis
Samantha Burchell

Policy and Research Officers

Joanna Carr
Claire Downey
Daniel Evans
Sonia Magri
Siobhan McCann
Dr Zoë Morrison
Priya SaratChandran

Communications Officers

Alison Hetherington
Trish Luker

Project Officer

Simone Marrocco

Librarian

Julie Bransden

Administrative Officers

Vicki Christou/Failelei Siatua
Lorraine Pitman

* 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

| | |
|--------|--|
| AFL | Australian Football League |
| AHEC | Australian Health Ethics Committee |
| AIRC | Australian Industrial Relations Commission |
| ALRC | Australian Law Reform Commission |
| art | article |
| CCTV | closed-circuit television |
| ch | chapter |
| cf | compare |
| Cth | Commonwealth |
| DEWR | Department of Employment and Workplace Relations |
| div | division |
| DNA | deoxyribo nucleic acid |
| ed | edition |
| (ed/s) | editor/s |
| EOCV | Equal Opportunity Commission Victoria |
| GPS | global positioning system |
| HCA | High Court of Australia |
| HIV | human immunodeficiency virus |
| ibid | in the same place (as the previous footnote) |
| ie | that is |
| ICCPR | International Covenant on Civil and Political Rights |
| ILO | International Labour Office |
| J | Justice |

| | |
|----------------|---|
| n | footnote |
| no | number |
| NRL | National Rugby League |
| NSW | New South Wales |
| NSWLRC | New South Wales Law Reform Commission |
| NZCA | New Zealand Court of Appeal Reports |
| OHS | occupational health and safety |
| para/s | paragraph/s |
| pt | part |
| RFID | Radio Frequency Identification |
| s | section (ss plural) |
| sch | schedule |
| sess | session |
| SMS | short message service |
| UN GAOR | United Nations General Assembly |
| UN Res | United Nations resolution |
| v | and (civil) or against (criminal) |
| VCAT | Victorian Civil and Administrative Tribunal |
| Vic | Victoria |
| VoIP | voice over internet protocol |
| vol | volume |
| WADA | World Anti-Doping Agency |

Executive Summary

PURPOSE OF THE FINAL REPORT

Long-held assumptions about privacy are being challenged daily by the onslaught of rapidly advancing technologies. The impacts of these technologies are being felt in all spheres of public life and the workplace is no exception. More and more workers are being subjected to various forms of surveillance, monitoring and testing. In the past, if an employer wanted to monitor or assess a worker's performance or behaviour it would have involved some form of personal observation. Employers now have access to technology and medical science that allows them unprecedented access into workers' lives.

The right to privacy is a fundamental human right, recognised in international law, to which all people are entitled. This includes workers. Privacy rights direct our attention to the importance of autonomy and dignity in our everyday lives—and recognise not only the privacy of individuals, but privacy as a value to society as a whole.

However, like other human rights, privacy is not an absolute right. The way in which it is protected and regulated within the workplace must be balanced against other important social interests, such as allowing employers to manage their businesses productively and safely. Do current laws respond to the challenges and balance interests in a way that reflects community expectations?

In the commission's view, workers' privacy is not adequately protected. There are significant legislative gaps in relation to the protection of privacy in workplaces, particularly in light of the federal employee records exemption which generally excludes protection of private-sector employees' personal information. The commission has concluded that these gaps require regulation at the state level. Such regulation is necessary if we are to provide meaningful privacy protection in accordance with our international obligations.

To achieve this, the commission believes the best approach is to address the acts or practices of employers that occur before any information is created (eg the practices of surveillance or testing of workers). This preventative approach differs from existing federal and state privacy legislation, which focus on protecting information obtained through acts or practices.

PROPOSED MODEL

We believe Victoria's workplace privacy inquiry is the first of its kind in the world. Our proposed legislative model aims to provide the necessary balance between the interests of employers, workers, and the wider community.

It became apparent to the commission from roundtable discussions and submissions that people view some practices as being more intrusive than others. The commission's approach is to ensure that the level of regulation it recommends is responsive to, and corresponds with, the level of intrusion into people's lives.

Our recommended legislative model gives workers greater privacy protection outside the work context than they will receive while they are working. This distinction reflects the differing balance between employers' interests and workers' expectations of privacy in these two contexts. Under our model, if an employer does not engage in privacy-invasive acts and practices, then the regulatory impact on the employer's business is nil. Conversely, employers are regulated only to the extent to which they choose to use privacy-invasive acts or practices in their businesses.

The commission proposes the creation of workplace privacy legislation which will provide a comprehensive 'one-stop-shop' for the regulation of potentially privacy-invasive acts and practices in the workplace. The proposed legislation has been included in this report.

Under our proposed model, an independent regulator will be appointed to oversee the operation of the legislation and investigate and resolve complaints about privacy breaches.

LIGHT-TOUCH REGULATION—WORK-RELATED ACTIVITIES

Regulation which is not intrusive or prescriptive and which is cheap to administer and comply with is often described as 'light touch'. Under our proposed legislation, light-touch regulation will apply to most practices which affect workers when they are involved in work-related activities.

EMPLOYER OBLIGATION

Our proposed legislation imposes an obligation on employers not to unreasonably breach the privacy of prospective workers or workers while they are working. The legislation includes a set of principles and makes provision for the making of advisory, approved and mandatory codes by a regulator appointed under the legislation.

Principles

The principles will assist employers in complying with the general obligation described above. Thus, an employer will unreasonably breach the privacy of a worker where an act or practice is performed or carried out:

- for a purpose not directly connected to the employer's business;
- in a manner that is not proportionate to the purpose for which the act or practice is undertaken;
- without first taking reasonable steps to inform and consult with workers;
- without providing adequate safeguards to ensure the act or practice is conducted appropriately, having regard to the obligation to not unreasonably breach workers' privacy.

The way in which this scheme will work can be illustrated by the following practical example.



CASE STUDY

Marcella works from home for a software developing company. Once a week, Marcella goes to the company's offices to attend internal meetings and meet with clients. One week Marcella attends the staff meeting, at which the director notifies staff that the company will be introducing overt video surveillance in the main foyer for security purposes. The director then informs Marcella and her colleagues that at the conclusion of the meeting the company will conduct a random alcohol and drug test as part of its occupational health and safety program.

Marcella's company will be subject to the general obligation not to unreasonably breach the privacy of its workers under the proposed legislation. On the face of things, its overt video surveillance may well be consistent with this general obligation if the company has consulted with and notified workers of the overt video surveillance, and if the placement of the cameras is restricted to security-sensitive areas. In such circumstances, the way the practice is carried out may not be disproportionate to its purpose. However, the company's use of random drug and alcohol tests might be less clear, and further guidance to employers in making this assessment is provided for through the development of codes of practice.

Advisory and Approved Codes of Practice

The regulator will have the power to issue advisory codes of practice to provide guidance on the content of employers' obligations, or to approve codes developed by employers. Codes will indicate how employers should undertake particular acts or practices. If the regulator issued an advisory code on overt video surveillance, Marcella's company would be able to use it to develop its own company policy and processes.

If a worker or prospective worker complains about a privacy-invasive practice covered by an advisory code, the complaint will not be upheld if the employer has followed a relevant advisory code of practice. If Marcella's company has complied with the advisory code of practice on overt surveillance, it will have complied with its obligation. If the company has contravened the advisory code of practice, it will have contravened the Act, unless it can establish that it has met its obligation in some other way.

Unlike advisory codes of practice, failure to comply with an approved code (which has been prepared by an employer) will be a contravention of the employer's obligation not to unreasonably breach the privacy of workers.

If the regulator believes employers are failing to meet their obligations under the light-touch regulatory regime (eg under particular advisory or approved codes) the regulator may recommend that the practice in question be prescribed and made subject to more onerous (mandatory) regulation.

The obligation and principles continue to apply to employers, regardless of whether or not a code is in place.

Mandatory Codes of Practice

The regulator will be required to produce certain codes of practice (mandatory codes) to govern activities affecting workers which are particularly privacy invasive. These include covert surveillance of workers while they are working and taking bodily samples from workers or prospective workers to test for the presence of drugs and alcohol. If the company's occupational health and safety program includes random alcohol and drug testing, it must comply with the relevant mandatory code of practice.

Failure to comply with a mandatory code will be a breach of the employers' obligation not to unreasonably breach workers' privacy. If Marcella's company has not complied with the requirements of the relevant mandatory code on drug and

alcohol testing and a complaint is made, the assumption will be that the company has breached its workers' privacy.

STRICTER CONTROLS FOR SERIOUS PRIVACY INTRUSIONS

Although the commission supports light-touch regulation to deal with most aspects of workplace privacy, we do not believe codes of practice can provide sufficient protection against some practices which seriously affect workers' privacy. In the commission's view, stricter controls should apply to acts or practices which affect workers' privacy in the following circumstances: where they are not working and where they are subjected to genetic testing. In addition, there are some acts and practices which require even stricter regulation.

EMPLOYER OBLIGATION

In this context, an employer must not engage in acts and practices without meeting the regulatory requirements of the legislation. Unlike the employer's obligation relating to work-related activities, there is no provision made for whether a privacy breach is 'unreasonable' or 'reasonable'. This obligation will apply to certain activities requiring authorisation (non-work-related activities, genetic testing). Some activities will be prohibited outright (eg surveillance in private areas of the workplace).

Authorisation for Non-work-related Activities



CASE STUDY

Marcella's company decides to start monitoring all workers' email content, including outworkers like Marcella. In the course of this monitoring, Marcella's supervisor discovers she is receiving and sending emails very late at night containing explicit sexual material. The company is also considering introducing web camera attachments to all workers' computers as a productivity measure.

Regulator authorisation will be required in advance if a practice affects workers while they are not working, for example out-of-hours surveillance of a worker who is suspected of theft. The company's proposal to introduce web cameras on all computers would entail seeking an authorisation where, as in Marcella's situation, workers use their computer at home.

There is one exception to this out-of-hours rule. An employer will not be required to obtain an authorisation before monitoring the workers' use of the employer's communications system, regardless of whether the worker is based at home or elsewhere. Instead, use of the employer's communication system is deemed a 'work-related activity' under the model, and will be regulated in accordance with an advisory code of practice. As such, the company's policy on random monitoring will be regulated by an advisory code, despite Marcella using the communication system from home, late at night. The company will not need to seek an authorisation to monitor in these circumstances.

Authorisation for Genetic Testing



CASE STUDY

Marcella's company is considering whether it should expand its occupational health and safety program to include staff DNA testing to ascertain a predisposition or existing genetic condition that could give rise to a WorkCover claim. Marcella has a genetic condition that gradually affects her eyesight. This can be exacerbated by prolonged computer use.

We also propose that stricter controls apply to activities which affect the bodily integrity of workers or prospective workers. It is the commission's view that genetic testing and should require regulator authorisation before it can be carried out. The legislation will allow authorisation requirements to be extended to new technologies which have a significant impact on workers' privacy. If Marcella's company wishes to introduce DNA testing as part of its occupational health and safety program, it will need to seek prior authorisation from the regulator.

Prohibition of Certain Activities



CASE STUDY

Marcella was not aware that when she went to the office bathroom to provide a sample for the random alcohol and drug test after the staff meeting she was being filmed. The company had installed hidden cameras in the bathroom to ensure staff were not diluting their samples.

The commission believes stricter controls are warranted where a practice seriously demeans human dignity. Surveillance in private areas in the workplace, for example in toilets and bathrooms, will be prohibited. These are areas in which all members of the community have a particularly high expectation of privacy. Placing workers under surveillance in these areas would have an unacceptable effect on their sense of dignity and autonomy. The company's covert filming of Marcella and her colleagues while they were in the bathroom violates the prohibition under the proposed legislation.

FUNCTION OF THE REGULATOR AND COMPLAINTS PROCESSES

One of the main roles of the regulator will be to promote understanding of and compliance with the legislation. Education of employers and workers will ensure they understand their rights and responsibilities under the proposed legislation.

The legislation allows for Marcella and her colleagues to complain to the regulator about an alleged breach of privacy. Unions and professional associations can also make complaints on behalf of members.

However, the commission believes the proposed model will only provide adequate privacy protection if the regulator is able to go beyond dealing with individual complaints and can take a more systemic approach to workplace privacy issues. We therefore recommend the regulator have the power to undertake two different kinds of systemic investigation:

- to investigate matters other than the breach which is the subject of complaint;
- to conduct inquiries and publish reports on issues relating to workplace privacy.

Under these powers, if the regulator becomes aware of other breaches while investigating an act or practice, the regulator is then able to initiate an investigation into this act or practice. In Marcella's case, if the regulator learns of plans to install web cameras on workers' computers while investigating the bathroom surveillance breach, the regulator could initiate an investigation to address the use of the web cameras.

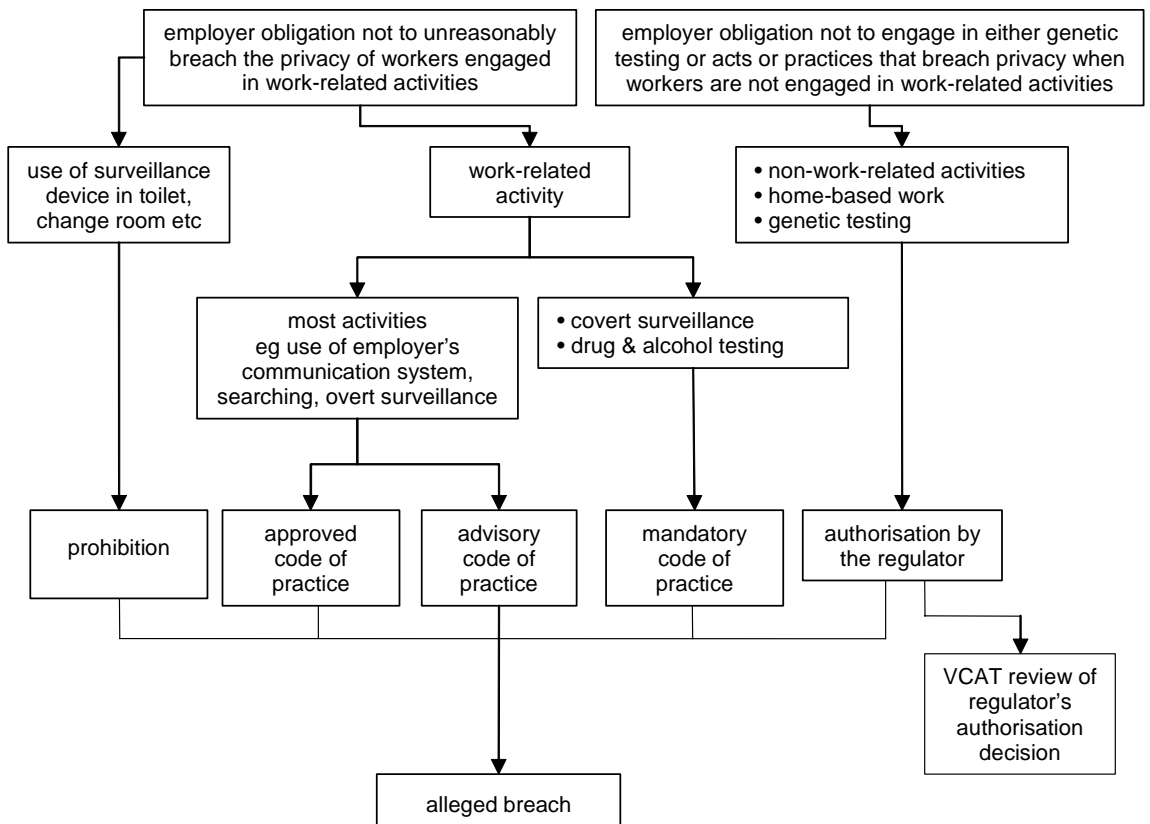
The regulator is also able to conduct an inquiry if, for example, he or she believes that the overt surveillance advisory code used by the software industry is being disregarded by employers. At the conclusion of an inquiry, the regulator will be able to make recommendations to the relevant government minister, such as

recommending that overt surveillance become subject to a mandatory code of practice.

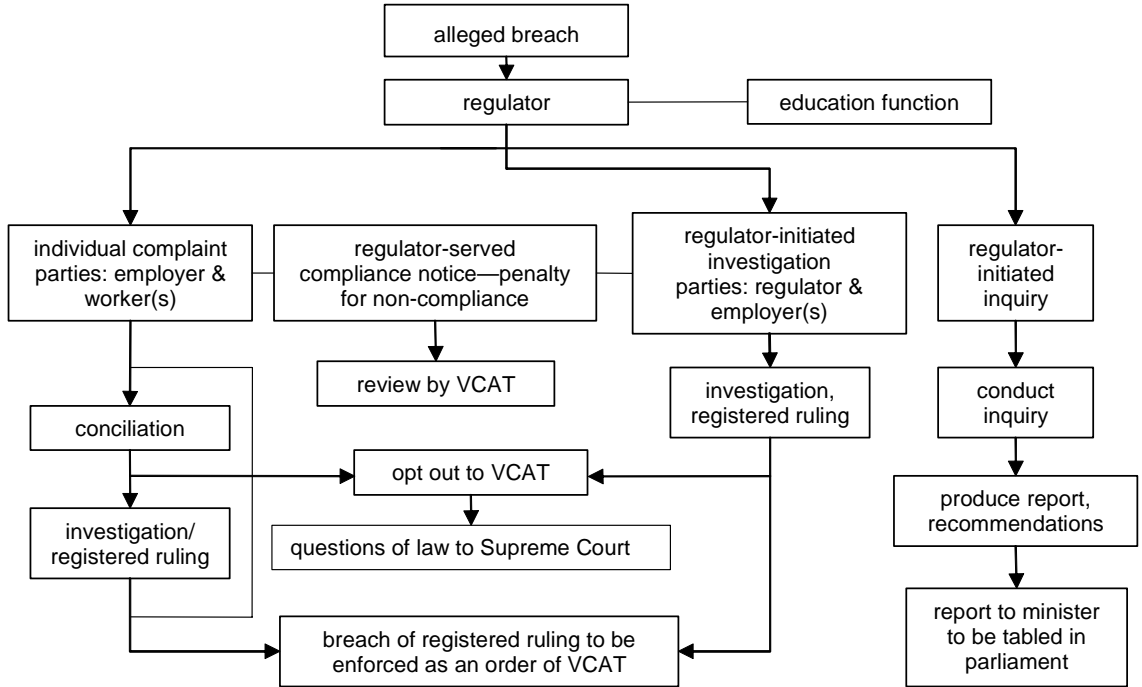
We also recommend that the proposed legislation prohibit victimisation. If an employer retaliates, or threatens to retaliate, against a worker or prospective worker who has made a complaint or taken other action under the legislation, the worker will be able to complain to the regulator.

Following are two flowcharts which illustrate the processes involved in guiding employers on their obligations and what happens if a worker’s privacy is breached.

EDUCATION AND GUIDANCE



PRIVACY BREACHES



Recommendations

Chapter 3

1. The legislation should provide that an employer must not engage in acts or practices that unreasonably breach the privacy of prospective workers or workers engaged in work-related activities.
2. An employer unreasonably breaches the privacy of prospective workers or workers if it engages in acts or practices:
 - for a purpose that is not directly connected to the employer's business;
 - in a manner that is not proportionate to the purpose for which those acts and practices are being used;
 - without first taking reasonable steps to inform and consult workers about the relevant act or practice;
 - without providing adequate safeguards to ensure the act or practice is conducted appropriately, having regard to the obligation not to unreasonably breach the privacy of the worker.
3. An act or practice is 'proportionate' under Recommendation 2 if it is the least privacy-invasive measure by which the intended purpose can be achieved.
4. The obligation to take reasonable steps to inform workers under Recommendation 2 requires provision of information to workers about:
 - the nature of the act or practice and the reasons for introducing it;
 - the number and categories of worker likely to be affected;
 - the time when, or the period over which, the employer intends to engage in the act or practice;
 - the alternatives considered and the reasons why the alternatives were not considered appropriate;

- the safeguards used to ensure the acts or practices are conducted appropriately.
5. The employer must take reasonable steps to give workers a genuine opportunity to influence the decision to introduce the act or practice.
 6. The regulator should have the power to issue advisory codes of practice to provide practical guidance to employers about how to fulfil the obligation imposed by Recommendation 1.
 7. Advisory codes may cover acts or practices which affect the privacy of workers or prospective workers while they are engaged in work-related activities other than:
 - acts or practices to which mandatory codes apply under Recommendation 14;
 - acts or practices which require authorisation under Recommendations 19, 22 and 25.
 - acts or practices which are prohibited under Recommendation 30.
 8. An advisory code of practice prepared by the regulator must be consistent with the principles in Recommendation 2.
 9. Compliance with an advisory code is conclusive evidence that the employer has complied with the obligation imposed by Recommendation 1.
 10. If an advisory code is in operation, contravention of the code is a contravention of the obligation imposed by Recommendation 1 unless the employer complies with that obligation in some other way.
 11. The regulator should have the power to approve codes of practice (approved codes) prepared by employers that deal with acts or practices that affect the privacy of workers while they are engaged in work-related activities, other than:
 - acts or practices to which mandatory codes apply under Recommendation 14;
 - acts or practices which require authorisation under Recommendations 19, 22 and 25;
 - acts or practices which are prohibited under Recommendation 30.

12. The regulator may only approve a code which is consistent with the principles set out in Recommendation 2.
13. An employer must comply with an approved code of practice.
14. The regulator must issue mandatory codes of practice about the following acts or practices:
 - covert surveillance of workers in the workplace (including covert use of optical surveillance devices and of listening or tracking devices and covert surveillance or monitoring of emails or internet use);
 - the taking of bodily samples from workers or prospective workers for the purposes of drug and alcohol testing;
 - any other acts or practices that are prescribed by regulation for the purposes of this section.
15. A mandatory code of practice must be consistent with the principles in Recommendation 2.
16. In deciding whether to issue a mandatory code the regulator should consult with relevant organisations and persons.
17. A mandatory code of practice, or a variation or revocation of a mandatory code of practice, must be approved by the relevant minister.
18. An employer who fails to comply with a mandatory code breaches the obligation imposed by Recommendation 1.
19. The legislation should provide that an employer must not engage in acts or practices that breach the privacy of a worker when the worker is engaged in non-work-related activities without an authorisation from the regulator.
20. The regulator may authorise the employer to engage in an act or practice which affects the privacy of a worker engaged in non-work-related activities, if the regulator is satisfied that:
 - there are reasonable grounds for believing the worker's out-of-hours activity may have a direct and serious impact on the business or reputation of the employer;
 - the employer's act or practice affecting privacy cannot reasonably be undertaken while the worker is engaged in work-related activities;

- the act or practice is a proportionate response to the protection of the employer's interests;
 - the employer will inform and consult workers concerning the act or practice and ensure the act or practice is conducted appropriately;
 - adequate safeguards have been put in place to minimise breaches of workers' privacy.
21. An employer may seek a review by VCAT of the regulator's decision to authorise or refuse to authorise.
22. An employer must not use acts or practices which affect workers' privacy while they are working at home, unless the act or practice is authorised by the regulator.
23. The regulator may authorise an employer to use acts or practices which affect the privacy of workers while they are working at home if the regulator is satisfied of the matters set out in Recommendation 20.
24. An employer should not be required to seek an authorisation to monitor a worker's email or internet use when the worker is using the employer's communication system, wherever the worker is situated.
25. An employer must not conduct genetic testing of workers or prospective workers unless genetic testing is authorised by the regulator.
26. The regulator may authorise an employer to undertake genetic testing of workers if the regulator is satisfied that:
- workers have consented to being genetically tested;
 - there is substantial evidence of a connection between the working environment/workplace hazard and the existence or predisposition to a condition which may be detected using genetic testing;
 - the condition or predisposition which may be detected has the potential to seriously endanger the health and safety of the worker or a third party;
 - there are no other reasonable means by which the hazard, which genetic testing seeks to eliminate or reduce, can be eliminated or reduced;
 - there are no other reasonable means of detecting a condition;

- the proposed genetic test is scientifically reliable;
 - the employer has put in place adequate safeguards to ensure tests are conducted appropriately;
 - the employer has taken appropriate steps to ensure any information obtained as a result of the test will be adequately protected from disclosure;
 - the employer has taken reasonable steps to inform and consult with workers about the conditions under which the genetic testing will be undertaken.
27. Genetic testing means the use of samples obtained from the body of a worker, or prospective worker, for the purposes of obtaining genetic information about the worker or prospective worker.
 28. The legislation should provide for regulations to be made requiring other acts or practices which have a serious effect on workers' privacy to be authorised before they can be used by employers.
 29. The regulator should establish a system for expediting authorisation applications in urgent cases.
 30. An employer should be prohibited from using any device to observe, listen to, record or monitor the activities, conversations or movements of a worker in toilets, change rooms, lactation rooms, wash rooms or in any other prescribed circumstances.
 31. Acts or practices of employers which involve installation, use or maintenance of surveillance devices in relation to their workers should be regulated by the Workplace Privacy Act. The Surveillance Devices Act should be amended accordingly.
 32. The Department of Justice should consult with government agencies and statutory entities to determine whether statutory provisions in other legislation which affect workplace privacy should be repealed or retained.

Chapter 4

33. A statutory office of the workplace privacy regulator should be established.

34. The workplace privacy regulator should be appointed by the Governor in Council for a term not exceeding seven years and should only be able to be removed from office for misbehaviour or incapacity.
35. The office of the workplace privacy regulator should be a 'special body' and the workplace privacy regulator should have the functions of an agency head in relation to employees according to the *Public Administration Act 2004*.
36. The workplace privacy regulator should be required to report annually to parliament.
37. The workplace privacy regulator should also have the power to report to the relevant minister on matters relating to his or her functions under the workplace privacy legislation. The minister should be required to table these reports in parliament.
38. The main functions of the workplace privacy regulator are to:
 - promote understanding of and compliance with the workplace privacy regime;
 - provide educational programs to promote understanding of the workplace privacy regime;
 - provide advice to any person or organisation on compliance with the legislation;
 - issue guidelines on the development of approved codes of practice prepared by employers or groups of employers;
 - receive complaints about an act or practice of an organisation that may contravene the workplace privacy legislation and investigate, conciliate and make rulings on complaints;
 - conduct audits of acts or practices of an employer to ascertain whether the employer is complying with obligations under the workplace privacy legislation;
 - monitor and report on the adequacy of equipment and system safeguards put in place to minimise the effect of acts or practices on workers' privacy;
 - conduct an investigation beyond the terms of a particular complaint;

- conduct an inquiry into acts or practices which affect workers' privacy;
 - assess any proposed or existing legislation that may adversely affect the privacy of workers or otherwise contravene the provisions of the Act, including reporting to the minister the results of assessment;
 - make public statements in relation to any matter affecting workplace privacy;
 - undertake research into and monitor developments affecting workplace privacy.
39. The regulator should have the power to investigate acts or practices of an employer which come to the regulator's attention while dealing with a complaint, in order to deal with privacy breaches of the same or a different kind as the breach which is the subject matter of the complaint.
 40. In exercising the function to conduct an inquiry, the regulator should have the power to obtain information and documents and examine witnesses.
 41. In exercising the function to audit and monitor, the regulator should have the power to obtain information and documents, examine witnesses and to enter premises.
 42. A worker or prospective worker should be able to complain to the regulator about an act or practice that may be a breach of the legislation.
 43. Where an act or practice breaches the privacy of two or more workers, any one of them should be able to complain to the regulator on behalf of all workers who are affected, with their consent.
 44. A representative body should be able to complain to the regulator on behalf of a worker or workers if that body has sufficient interest in the complaint.
 45. A representative body should be regarded as having sufficient interest in the complaint if the conduct is a matter of concern to the body because of its effect on the interests of the body or the privacy of the person it represents.
 46. The regulator should have the power to receive complaints about possible breaches of the legislation and to decline or accept them.
 47. If the regulator decides to accept a complaint it may attempt to resolve it informally.
 48. The regulator may decline a complaint if:

- the act or practice about which the complaint has been made is not a breach of the individual's privacy;
- the complaint is made on behalf of a complainant by a person not authorised to do so;
- the complaint to the regulator was made more than 12 months after the complainant became aware of the act or practice;
- the complaint is frivolous, vexatious, misconceived or lacking in substance;
- the act or practice is the subject of
 - (i) an application under another enactment; or
 - (ii) a proceeding in a court or tribunal

and the subject-matter of the complaint has been, or is being, dealt with adequately by that means;

- the act or practice which is the subject of the complaint could be more appropriately dealt with under another enactment;
- the act or practice is subject to an applicable code of practice or authorisation and mechanisms available for seeking redress under that code or authorisation have not been exhausted;
- the complainant has complained to the respondent about the act or practice and either
 - (i) the respondent has dealt, or is dealing, adequately with the complaint; or
 - (ii) the respondent has not yet had an adequate opportunity to deal with the complaint.

49. If the complaint is accepted the regulator may:

- attempt to resolve the matter informally;
- conciliate the complaint if appropriate;
- investigate the complaint and, if appropriate, make a ruling as to whether there has been a breach of privacy and set out any action which the regulator requires the employer to undertake to remedy the complaint.

50. A ruling may provide that:
 - the employer must not repeat or continue the conduct;
 - the employer must perform any reasonable act or undertake a course of conduct to redress any loss or damage suffered by the worker;
 - any existing authorisation the employer possesses be revoked, or revoked until the employer takes specified action;
 - the employer publish, at the employer's expense, an advertisement as specified in the order (the regulator may also publish details of the employer's conduct and/or number of complaints in its annual report).
51. Where the act or practice affects people other than the person making the complaint, the regulator may make a ruling to protect the privacy of people other than the person making the complaint, if having regard to the circumstances it is appropriate to do so.
52. If the respondent fails to comply with a ruling and does not seek to refer the matter to VCAT for hearing, the complainant can register the ruling with VCAT. On registration, the ruling is to be taken as an order of VCAT and can be enforced accordingly.
53. The legislation should prohibit victimisation of workers (including prospective workers) by the employer.
54. An employer victimises a worker (including prospective workers) if the employer subjects or threatens to subject the worker to any detriment because the worker, or a person associated with the worker:
 - has made a complaint against the employer under the Act;
 - has given evidence or information, or produced a document, in connection with any proceedings under the Act;
 - has attended a conciliation conference;
 - has alleged that the employer has contravened the Act, unless the allegation is false and was not made in good faith;
 - has refused to do something that would contravene a provision of the Act;

- because the worker has reasonable cause to believe the employer has done or intends to do any of the above.
55. The legislation should impose a civil penalty for:
- performing an act which is prohibited;
 - failing to report to the regulator about action taken in response to a ruling;
 - not seeking an authorisation for an act or practice which affects the privacy of workers while they are engaged in non-work-related activities;
 - breaching an authorisation for an act or practice that affects the privacy of workers while they are engaged in non-work-related activities;
 - not seeking an authorisation or breaching an authorisation for genetic testing.
56. Where an employer fails to comply with a ruling made by the regulator or the employer has performed an act or used a practice which is a serious or flagrant contravention of the workplace privacy legislation, the regulator should have the power to serve a compliance notice on the employer.
57. The compliance notice may require the employer to refrain from an act or practice or to take specified action within a specified period of time and to report the taking of that action to the regulator.
58. A civil penalty should apply for failure to comply with a compliance notice.
59. The regulator should have the additional power to view premises and equipment where a ruling has been made or a compliance notice issued to ensure the employer is satisfying its obligations.
60. VCAT should have jurisdiction to hear a complaint when:
- the regulator declines to entertain a complaint and the complainant requires the regulator to refer the matter to VCAT for a hearing of the complaint;
 - the regulator decides that conciliation is inappropriate and decides not to further entertain the complaint and the complainant requires the regulator to refer the matter to VCAT;

- conciliation fails and the complainant requires the regulator to refer the matter to VCAT;
 - the regulator makes a ruling and a complainant or respondent requires the regulator to refer the matter to VCAT.
61. Where, after a hearing, VCAT finds that a complaint is substantiated, it may make an order that:
- the employer must not repeat or continue the act or practice;
 - the employer must perform any reasonable act or undertake a course of conduct to redress any loss or damage suffered by the worker;
 - the worker is entitled to a specified amount not exceeding \$100,000 as compensation for any loss or damage suffered, including injury to the worker's feelings or humiliation suffered by the worker as a result of the employer's act or practice;
 - the employer publish, at the employer's expense, an advertisement as specified in the order;
 - any existing authorisation the employer possesses be revoked, or revoked until the employer performs another specified act.
62. Where the act or practice affects people other than the person making the complaint, VCAT may make a ruling to protect the privacy of people other than the person making the complaint if, having regard to the circumstances, it is appropriate to do so.
63. VCAT should have the jurisdiction to review a decision by the regulator to issue a compliance notice.
64. VCAT should have the jurisdiction to make interim orders to prevent a party to a complaint from acting in a way which is prejudicial to conciliation or to any decision or order VCAT may subsequently make.
65. The Supreme Court's jurisdiction to hear appeals on questions of law from VCAT should apply to decisions under the workplace privacy legislation.

Chapter 1

Introduction

OUR TERMS OF REFERENCE

1.1 This is the Victorian Law Reform Commission's Final Report into workplace privacy. 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.

1.2 The terms of reference require us to examine a wide range of activities which may affect workers, including: surveillance by video, audio or tracking devices; monitoring of email and internet use; physical and psychological testing; searching workers and their belongings; and the handling of personal information. We were also asked to consider how new technologies affect workers' privacy. Our terms of reference define 'workers' broadly, to cover 'employees, independent contractors, outworkers and volunteers'.

1.3 The breadth of the terms of reference distinguishes this project from other Australian inquiries relevant to workers' privacy, most of which have focused on use of surveillance. For example, in 2001 the New South Wales Law Reform Commission (NSWLRC) delivered its interim report on surveillance, which resulted in enactment of the *Workplace Surveillance Act 2005* (NSW).¹ We believe our project is the first in the world to consider all aspects of workers' privacy, though other jurisdictions have considered some of the practices discussed in this report.

1.4 In the next phase of our project we will make recommendations on surveillance in public places.²

1 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No 98 (2001).

2 See the terms of reference on p viii.

PURPOSE OF THIS REPORT

1.5 The *Workplace Privacy: Issues Paper*, published in 2002, explained the reasons the commission had been asked to examine the adequacy of laws affecting workers' privacy.³ In the past, if an employer wanted to monitor a worker's performance or behaviour this usually involved some form of personal observation. Those days are gone. Rapid developments in technology and medical science have created an unprecedented ability to observe, monitor and test individuals. Throughout the course of this reference, newspapers have reported almost daily on issues affecting privacy within the workplace.

1.6 In Chapter 2 of this Final Report, we discuss why reform of laws affecting workers' privacy is necessary. We argue that existing laws do not provide a fair balance between employers' interests and workers' privacy. The purpose of this report is to propose a regulatory model that achieves this balance and provides certainty for both employers and workers about practices that affect privacy and when it is appropriate to use them.

1.7 Appendix 5 of this report includes a Workplace Privacy Bill, which was drafted for the commission by the Office of Parliamentary Counsel. The Bill contains provisions on administration and enforcement processes which are not discussed in detail in the report. The Law Commission of England and Wales has commented that:

Drafting Bills does not involve a simple transformation of policy decisions into legislative form. Ideas which may seem straightforward to policy-makers may be hard, if not impossible, to translate into legislative form.⁴

Drafting of the Bill enabled the commission to critically examine and refine our policy ideas. We are most grateful for the role played by the Office of the Chief Parliamentary Counsel in the production of this report.

OUR APPROACH TO THE REFERENCE

DEFINING PRIVACY

1.8 The commission's Issues Paper discussed the difficulty of defining privacy as a precise legal concept. Despite this difficulty, privacy is recognised as a human right in

3 Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (October 2002) para 1.2.

4 The Law Commission [UK], *Renting Homes: Report on a Reference Under Section 3(1) (e) of the Law Commission Act 1965*, LAW COM No 284 (2003) 1.

international law⁵ and in various constitutional bills of rights.⁶ It is also clear that Australians regard privacy as an important social value.⁷

1.9 While there is no enforceable right to privacy in domestic law, courts have recognised privacy as a value which underpins a number of legal principles. In the High Court case of *Australian Broadcasting Corporation v Lenah Game Meats*,⁸ Chief Justice Gleeson commented that, ‘The law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy’.⁹

1.10 In the English House of Lords case of *Wainwright v Home Office*, Lord Hoffman said that although there is no single legal wrong (tort) of invasion of privacy, privacy is a value which underlies a number of specific legal principles and directs their development.¹⁰

1.11 Similarly, in a recent New Zealand case the majority of judges did not offer a comprehensive definition of privacy, but examined the circumstances which give rise to a ‘reasonable expectation of privacy’. One of the majority judges said:

5 *International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), UN GAOR, 21st sess, UN Doc A/6316 (1966), 999 UNTS 171, entered into force 23 March 1976, art 17, <www.austlii.edu.au/au/other/dfat/treaties/1980/23.html> at 3 August 2005. Article 12 of the *Universal Declaration of Human Rights* refers to privacy in almost identical terms to the ICCPR, and Article 16 of the *Convention on the Rights of the Child* applies these terms specifically to the rights of children: *Universal Declaration of Human Rights*, UN GA Res 217A (III), UN GAOR 3rd sess, UN Doc A/810 at 71 (1948), <www.un.org/Overview/rights.html> at 3 August 2005; *Convention on the Rights of the Child*, UN Res 44/25, UN GAOR, 44th sess, UN Doc A/44/736 (1990), <www.austlii.edu.au/au/other/dfat/treaties/1991/4.html> at 3 August 2005.

6 Countries whose citizens have express constitutional rights to privacy or bills of rights containing rights to privacy include Argentina, Belgium, Brazil, Bulgaria, Chile, China, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Peru, the Philippines, Poland, Portugal, Russian Federation, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine and United Kingdom. The United States has the so-called penumbra right of privacy: while there is no express privacy provision in the Constitution, the Supreme Court has ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights: see Marc Rotenberg and Cedric Laurant, *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Development* (2000) <www.privacyinternational.org/survey> at 22 August 2005.

7 See, eg, Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004).

8 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63 (Unreported, Gleeson CJ, Gaudron, Gummow, Kirby, Hayne and Callinana JJ, 15 November 2001).

9 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63 (Unreported, Gleeson CJ, Gaudron, Gummow, Kirby, Hayne and Callinana JJ, 15 November 2001) [40] (Gleeson CJ).

10 *Wainwright v Home Office* [2003] 3 WLR 1137, 1146.

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.¹¹

1.12 Privacy also receives some protection in federal and state legislation. The *Surveillance Devices Act 1999* (Vic) protects privacy by limiting the use of surveillance, and the *Information Privacy Act 2000* (Vic) and the *Health Records Act 2001* (Vic) recognise the interests of individuals in having the privacy of their personal and health information protected.¹² Information privacy is also protected by the *Privacy Act 1988* (Cth), subject to some exceptions.

1.13 The starting point for the regulatory scheme proposed in this Final Report is that privacy is a fundamental human right which is recognised in international law. However, as we explained in the Issues Paper, the purpose of recognising a right of privacy is not simply to protect the privacy of individuals but also to recognise that privacy has a value to society as a whole. Questions about how workers' privacy should be protected are linked to broader questions about the nature of our society and about the aspects of our humanity that should be protected from incursion.

1.14 In earlier discussions we said privacy includes:¹³

- 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;
- the right to establish and develop relationships with other people.

1.15 These rights reflect the link between privacy, personal autonomy and dignity. While this link is not sufficiently precise to provide a legislative definition of privacy, it directs attention to the central questions we have had to consider. How should the autonomy and dignity of workers be recognised and protected? How should these values be balanced against other important social interests, particularly the interest in allowing employers to manage their businesses safely and productively? What other factors should be taken into account in achieving an appropriate balance? The principles we have formulated (see Chapter 3) reflect these values as part of a range of

11 *Hosking & Hosking v Simon Runtig* [2004] NZCA 34, paras 249–50 (Tipping J, 25 March 2004).

12 *Information Privacy Act 2000* (Vic) s 1(d); *Health Records Act 2001* (Vic) s 1(a).

13 Kate Foord, *Defining Privacy* (2002) 3.

societal values or, as Chief Justice Gleeson put it in *Australian Broadcasting Corporation v Lenah Game Meats*¹⁴ the interests that constitute the concept of privacy.¹⁵ This ‘balancing of interests’ approach underpinned the two regulatory models proposed in the *Workplace Privacy: Options Paper*, published in 2004, which are discussed in more detail in Chapter 2 of this Final Report.

1.16 Both the Issues Paper and the Options Paper canvassed examples of the way that workers’ privacy may be affected by various acts and practices in the workplace. The Final Report does not include detailed case studies but focuses on explaining the features of our proposed model for regulating workplace privacy.

CONSTITUTIONAL CONSTRAINTS

1.17 In considering law reform in this area, the commission has had to take account of constitutional constraints on the exercise of state legislative powers. As we explained in the Options Paper, both the Commonwealth Parliament and the Victorian Parliament have overlapping constitutional powers to legislate on privacy and on industrial relations.¹⁶ In 1996, the Victorian Government referred the power to legislate on specified industrial relations matters to the Commonwealth, but this referral of powers did not include workplace privacy. Under section 109 of the Australian Constitution, if a Victorian Act is inconsistent with valid federal legislation it is overridden by federal law to the extent of that inconsistency. Federal legislation relevant to the issues considered in this report includes the Privacy Act, the *Workplace Relations Act 1996* and the *Telecommunications Interception Act 1979*.

1.18 The federal Privacy Act protects the privacy of personal information of Commonwealth public sector employees.¹⁷ It also protects the personal information of people who are not employees (such as consumers, independent contractors, volunteers and job applicants) in the private sector. However, small businesses are generally not covered by the Privacy Act.¹⁸ While the Privacy Act applies to the private sector, it does not protect private-sector employees’ personal information which:

14 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001).

15 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001), 40.

16 Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (September 2004) paras 1.34–1.35; Appendix 4.

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

18 ‘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

- relates directly to the employment relationship between an employer and a current or former private sector employee;
- is held by the employer in an employee record (this is known as the 'employee records exemption').¹⁹

1.19 The operation of the employee records exemption leaves a significant gap in the privacy protection of workers' personal information.

1.20 The Workplace Relations Act only allows 20 matters to be included in awards.²⁰ The federal government has recently announced its intention to reduce the matters which can be included in award provisions, though attempts to constrain the states' power to legislate on minimum employment conditions may be challenged by the states in the High Court.²¹

1.21 Constitutional advice obtained by the commission suggests that the employee records exemption in the Privacy Act and Workplace Relations Act provisions limiting the content of awards would not be regarded as inconsistent with state laws regulating 'broader aspects of the privacy of employees', such as provisions regulating the searching and testing of employees. The advice concludes:

not apply to businesses that provide a health service, except where the health information is held in an 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 another body corporate that carries on a business that is not a small business: *Privacy Act 1988* (Cth) s 6D(9).

19 *Privacy Act 1988* (Cth) s 7B(3). 'Employee records' are defined in section 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, employee's performance or conduct and leave entitlements, union membership and other types of personal information.

20 *Workplace Relations Act 1996* (Cth) s 89A. While there is the potential for an exceptional matters order pursuant to section 89A(7) of the Workplace Relations Act, few orders have been issued in practice.

21 See Mark Phillips, 'IR court showdown now "inevitable"', *The Australian*, 5 August 2005; Brad Norington and Matthew Denholm, 'States to fight IR takeover in court', *The Australian*, 6 August 2005.

Subject to further regulation at the Commonwealth level there is considerable scope for state parliaments to regulate some aspects of workplace privacy... 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 Commonwealth Acts, would have a greater chance of avoiding the operation of section 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 the Workplace Relations Act.²²

1.22 Although there may be no inconsistency between the Workplace Relations Act and the legislation proposed in this report, an inconsistency could arise between state legislation and a clause contained in a certified agreement between an employer and either a union or a group of employees, or a clause in an Australian Workplace Agreement between an employer and employee. For example, a clause in an agreement could contain provisions about the location of surveillance cameras or the use of alcohol and drug testing.²³ Such clauses are present in very few federal agreements but where they exist they have the force of federal law.²⁴ These provisions would override state legislation that attempted to cover the same ground, though only in relation to employees covered by the particular agreement.²⁵ Apart from this situation, states can legislate in the area of workplace privacy.²⁶ It should also be noted that our proposed workplace privacy scheme will protect the privacy of volunteers and independent contractors, who fall outside the scope of the federal Workplace Relations Act.

1.23 Another area of possible inconsistency arises between the federal Telecommunications Interception Act and provisions proposed in this report to cover

22 VLRC (September 2004), above n 16, Appendix 4, para 3.6.3. Advice provided by Amelia Simpson and James Stellios, Faculty of Law, Australian National University.

23 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. Electronic monitoring is covered 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). 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).

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

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

26 VLRC (September 2004), above n 16, Appendix 4, 3.3.5.

monitoring of email and internet use. The Telecommunications Interception Act covers an interception of a communication 'passing over the telecommunications system'.²⁷ 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 Act²⁸ and any inconsistent state law will be overridden. The constitutional advice already mentioned suggests the states can regulate processes that fall outside this definition, that is, processes of interception or monitoring of communications that occur prior to, or after, the communication has 'passed over the system'.²⁹ Recent amendments to the Telecommunications Interception Act³⁰ seem to confirm this view as it excludes 'stored communications' from the current prohibition against interception of communications.³¹ Stored communications include stored email, voicemail and SMS messages.³²

FOCUS ON PRACTICES RATHER THAN INFORMATION

1.24 The constitutional advice we received has helped shape our approach to this project. Unlike existing federal privacy legislation, our proposed legislative scheme regulates the 'acts or practices' of employers, for example the practices of surveillance,

27 For further explanation of 'passing over the telecommunications system' see VLRC (2002), above n 3, para 4.13.

28 VLRC (September 2004), above n 16, paras 1.3.1, 3.4.

29 Ibid, paras 1.4.1, 3.5

30 *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth).

31 See *Telecommunications (Interception) Act 1979* (Cth) s 7(2)(ad) which states that the prohibition contained in s 7(1) does not apply to 'the interception of a stored communication, so long as the interception happens during the 12-month period beginning at the commencement of this paragraph'.

32 See *Telecommunications (Interception) Act 1979* (Cth) s 7(3A) which states 'In paragraph (2)(ad), a stored communication is a communication that is stored on equipment or any other thing, but does not include: (a) a voice over Internet protocol (VoIP) communication; or (b) any other communication stored on a highly transitory basis as an integral function of the technology used in its transmission'. See also 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 VoIP communication or any 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) sch 1, cl 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.

monitoring and testing of workers, rather than protecting the information obtained through the use of these acts or practices. This differs from most other Australian privacy legislation that is concerned with the creation, use and handling of personal information about individuals. The focus on ‘acts and practices’ allows the commission to adopt a proactive regulatory approach rather than reactively dealing with the information that is created as a result of the use of such acts and practices.

1.25 As we discuss in Chapter 2, significant gaps exist in workers’ privacy protection³³ and our consultations with employer and worker representatives revealed a level of uncertainty about what employers can and cannot do.

PROTECTION OF WORKERS’ INFORMATION UNDER PROPOSED REGIME

1.26 As we have explained, recommendations in this report deal with the use of practices to collect information about workers’ behaviour or characteristics, rather than with the protection of the information obtained by use of those practices. We recognise, however, that there are significant gaps in protection of the privacy of workers’ information. Concerns about these gaps were expressed during our consultations. For example, workers were concerned about use of surveillance tapes showing footage of workers and about who might have access to psychological test results.

1.27 The privacy of information about workers receives only piecemeal protection in Victoria. The Surveillance Devices Act makes it an offence to communicate or publish material about private conversations or private activities obtained from the use of surveillance or tracking devices, without the consent of each party involved.³⁴ However, this provision has limited application to workers, because most conversations and activities in workplaces will not come within the definition of private conversations and private activities.³⁵ The Information Privacy Act protects personal information of workers in the Victorian public sector but not of workers in the private sector. Health information of Victorian workers (both public and private sector) is protected by the Health Records Act.

1.28 In paragraph 1.18 we referred to the employee records exemption in the federal Privacy Act. Criticism of this exemption led the federal government to indicate that the

33 VLRC (October 2002), above n 3, paras 4.79–83, 4.105–111.

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

35 *Surveillance Devices Act 1999* (Vic) s 3.

exemption would be reviewed as part of a general review of the Privacy Act.³⁶ The Commonwealth Attorney-General's Department and the Department of Employment and Workplace Relations (DEWR) released *Employee Privacy: A discussion paper on information privacy and employee records* for public comment in February 2004. We have been informed by DEWR that a final report will be produced but will not be publicly released. At the time of publishing, DEWR was uncertain whether the report would be produced in 2005.³⁷

1.29 In the commission's view, it would be preferable to wait for an announcement from the federal government on the outcome of that review before a detailed option concerning information privacy for workers can be proposed.

1.30 If the federal government decides not to act in this area, the constitutional advice received by the commission suggests the Victorian Government could legislate to regulate collection and use of such information and that such legislation might not be found to be inconsistent with the employee records exemption in the federal Privacy Act.³⁸ The commission believes that if the federal government decides to retain the employee records exemption, the state government should give serious consideration to extending existing Victorian public sector information privacy protections to private sector employees. This will at least provide them with equivalent protection to that of public sector employees.³⁹ Failure to act would mean that public sector employees would continue to enjoy a higher level of privacy protection than private sector workers. The commission can see no reason for retaining this distinction.

WHO IS A WORKER?

1.31 Because privacy is a fundamental human right, our terms of reference require us to cover a broad range of work relationships. It would be inconsistent with this right to set up a 'caste system' of workers under which some people receive higher levels of

36 Options Paper, submission 20 (Appendix 3 has the full list of Options Paper submissions).

37 The commission was informed of this by DEWR, 15 July 2005.

38 See VLRC (September 2004), above n 16, Appendix 4, paras 3.1.9, 3.1.10. The Workplace Relations Act also contains regulations that deal with specific types of information held in employee records. This information is used primarily for ensuring that employers meet their obligations under applicable awards and agreements in facilitating the documenting of breaches of employer obligations (eg in the correct payment of wages). The Workplace Relations Act's regulations could impinge on the state's ability to legislate for employees, in so far as such regulations would override any state legislation found to be inconsistent with the operation of their provisions. The regulations, however, are limited in application to those workers covered by its provisions: *Workplace Relations Regulations 1996* (Cth) pts 9A, 9B.

39 See the provisions of the *Information Privacy Act 2000* (Vic).

privacy protection than others. A contractor working side-by-side with an employee in the same workplace should not receive a lower level of privacy protection. Other Victorian human rights based legislation, such as the *Occupational Health and Safety Act 2004*,⁴⁰ the *Accident Compensation Act 1985*⁴¹ and the *Equal Opportunity Act 1995*,⁴² include a broad range of workers.

1.32 Accordingly, throughout this report the term ‘worker’ includes both employees and other people in work relationships, such as independent contractors, outworkers and volunteers. In some contexts (eg drug and alcohol testing) job applicants are also covered. The term ‘employer’ is used to describe a person or organisation who engages another person to perform work or to work as a volunteer.⁴³

OUR PROCESS

1.33 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 the privacy of workers and canvassed possible approaches to reform. At 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.⁴⁴

1.34 The Options Paper identified gaps in workplace privacy protection and concluded that regulatory guidance was essential to balance workers’ and employers’ interests. Two regulatory models were proposed. The first option proposed a separate Act that required employers to seek authorisation from a regulator prior to conducting practices. The second option proposed a separate Act containing principles that employers would be required to follow when implementing practices. Under this option the regulator would produce codes to provide employers with practical guidance.⁴⁵

40 See definitions of ‘employee’, ‘self-employed person’ and ‘volunteer’ in the *Occupational Health and Safety Act 2004* (Vic) s 5.

41 See definition of ‘worker’ in the *Accident Compensation Act 1985* (Vic) s 5.

42 See definition of ‘employee’ in the *Equal Opportunity Act 1995* (Vic) s 4.

43 Peter Nygh and Peter Butt (eds) *Butterworths Australian Legal Dictionary* (1997) 414.

44 See VLRC (September 2004), above n 16, paras 1.14–1.19.

45 See VLRC (September 2004), above n 16, paras 4.63–4.65.

CONSULTATIONS

WHY CONSULT?

1.35 Inclusive and effective community consultation is an essential part of the law reform process. It is the community's perception of whether or not laws and law-making are legitimate that ultimately leads to them complying with their legal obligations. The commission believes that community consultation is an important way of facilitating people's input into the law reform process. It encourages transparency of processes and makes the commission publicly accountable for its recommendations.

CONSULTATION PROCESS

1.36 The commission has held consultations at a number of key stages of this project. Following the release of the Issues Paper, a consultation and submission round was initiated to seek the community's views on the issues identified and on the commission's proposed definition of privacy. We received 34 written submissions, mostly from organisations and representative bodies.

1.37 The commission also conducted roundtable discussions to gain further insight into privacy issues within Victorian workplaces and attitudes towards regulation. We consulted with a range of organisations which we considered formed a representative sample of the types of industries that used surveillance, monitoring and testing practices. We do, however, recognise the limitations of our consultation process, which has not covered every type of employer and worker.

1.38 We also met with a number of experts who aided our understanding of the technology involved in these practices and the forms of regulation these practices are currently subject to. We met with:

- individual employers;
- employer representative organisations;
- unions;
- experts in surveillance (video, audio, tracking and biometrics);
- members of medical and psychological representative organisations;
- experts on drug and alcohol testing;
- internet and email technology providers;
- lawyers from other related areas of law such as occupational health and safety, worker's compensation, industrial relations and equal opportunity law;

- representatives from Industrial Relations Victoria, Parliamentary Counsel and the Australian Privacy Foundation.

1.39 The Options Paper called for further submissions from members of the public—we received 36. Following the release of the Options Paper, a further consultation round was conducted to gain feedback on the two regulatory models proposed, attitudes to different types of regulation, and the strengths and failures of existing regulatory schemes/models. These views were taken into account by the commission in proposing the final model contained in this report. At this stage of the reference, we consulted with:

- employers;
- employer associations;
- unions;
- regulatory theorists;
- academics specialising in related areas of law;
- regulators from human-rights based jurisdictions;
- lawyers practising in related areas of law;
- technical experts on internet and email monitoring software and GPS tracking;
- the Australian Privacy Foundation;
- members of court and tribunal staff;
- sports associations;
- Parliamentary Counsel.

1.40 Throughout this process, the commission has also called on the members of the Workplace Privacy Advisory Committee, which is comprised of members with a broad range of expertise in the area of workplace privacy.

STRUCTURE OF THE REPORT

1.41 The structure of the remainder of this report is as follows:

- Chapter 2 outlines the case for reform as detailed in our Options Paper.
- Chapter 3 explains the commission's recommendations on the conceptual structure, obligations and principles contained in the proposed legislation.
- Chapter 4 sets out the enforcement regime for the legislation.

Chapter 2

The Case for Reform

INTRODUCTION

2.1 In this chapter we outline why we believe reform of the law is necessary to provide a proper evaluation and balancing of employer and worker interests. We then describe the feedback we received on the Options Paper and how this has led the commission to propose a model for the regulation of workplace privacy that is a hybrid of the two options in the paper.

PROTECTION OF PRIVACY AS A HUMAN RIGHT

2.2 The commission has approached this reference from a human rights perspective. Privacy is recognised as a basic human right under public international law. Article 17 of the *International Covenant on Civil and Political Rights* outlines the right to privacy in the following terms:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.⁴⁶

46 United Nations, *International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), UN GAOR, 21st sess, UN Doc A/6316 (1966), 999 UNTS 171 (entered into force 23 March 1976) <www.austlii.edu.au/au/other/dfat/treaties/1980/23.html> at 3 August 2005. Article 12 of the *Universal Declaration of Human Rights* refers to privacy in almost identical terms to the ICCPR, and Article 16 of the *Convention on the Rights of the Child* applies these terms specifically to the rights of children: *Universal Declaration of Human Rights*, UN GA Res 217A (III), UN GAOR 3rd sess, UN Doc A/810 at 71 (entered into force 10 December 1948), <www.un.org/Overview/rights.html> at 3 August 2005; *Convention on the Rights of the Child*, UN Res 44/25, UN GAOR, 44th sess, UN Doc A/44/736 (entered into force 2 September 1990), <www.austlii.edu.au/au/other/dfat/treaties/1991/4.html> at 3 August 2005. The Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11* opened for signature 11 May 1994, ETS 005, art 8 (entered into force 1 November 1998), <www.conventions.coe.int/treaty/en/treaties/html/005.htm> at 3 August 2005, also states '(1) Everyone has the right to respect for 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

2.3 The same right is formulated in similar terms in article 12 of the *Universal Declaration of Human Rights*. Australia is a signatory to both instruments.

2.4 There are constitutional limits on the powers of the Commonwealth Parliament to legislate comprehensively in relation to privacy matters. The focus of Commonwealth legislation to date has been on the creation, use and handling of personal information, or what is sometimes referred to as ‘information privacy’. Hence the protection of privacy at the Commonwealth level is less than complete.

2.5 The commission’s enquiries have revealed that significant legislative gaps exist in relation to the protection of privacy in workplaces. Information-gathering practices such as workplace surveillance, monitoring and testing are largely unregulated. The commission has concluded that these gaps require regulation at the state level. Such regulation is necessary if we are to provide meaningful protection of privacy in Australia in accordance with our international obligations. The focus of the commission’s inquiry has been on how the use of these practices might be best regulated within the workplace to safeguard the rights of workers, while at the same time taking into account the rights of employers to run their businesses.

2.6 Privacy is an important human right that is fundamental to a person’s autonomy and dignity. It needs to receive explicit recognition and protection in the workplace, just as other human rights such as bodily integrity and religious and political freedoms are protected through other forms of regulation, such as occupational health and safety and anti-discrimination legislation.

2.7 Although privacy is a human right, it cannot be seen as an absolute right in the sense of a right that is to be upheld in all circumstances.⁴⁷ It must be balanced against competing interests—those of the State and its agencies, as much as those of fellow citizens and the wider community. In the specific context of work, it is necessary to take into account the interests of employers in running their businesses. The commission has sought to devise a mechanism that will protect workers’ privacy effectively while taking into account the legitimate interests of employers. This balancing approach is similar to that already adopted in other federal and state laws dealing with human rights, notably anti-discrimination and equal opportunity laws.

economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

47 There is much written on whether there are any ‘absolute’ rights, see Jeremy Waldron (ed) *Theories of Rights* (1984).

ADVANCES IN TECHNOLOGY

2.8 The rate of technological change is an important consideration in framing a workplace privacy regulatory model. Such change has affected the workplace in two ways, particularly in the past decade. First, the way in which work is performed has changed dramatically. Secondly, new technology now provides unprecedented opportunities for employers to observe, monitor and test workers, not only in the performance of their work, but in areas of their lives that do not relate to their work. Some examples are:

- Global positioning system (GPS) technology, which enables an employer to track the movement of a vehicle, may also incidentally track the movements of the worker driving the vehicle after work.
- Monitoring technologies that enable employers to read workers' personal emails also apply to private correspondence sent through an organisation's system.
- Drug testing, which has a broad detection window with the potential of picking up the presence of legal as well as illegal drugs, and of detecting drug use which might not have occurred at the workplace or during work time.⁴⁸

An employer's use of technology may not only affect privacy in the workplace, but also has the potential to blur the distinction between a worker's activities at work and his or her private life.

2.9 It is very likely that the use of technology will increase as its capability and accessibility increases. During consultations it was noted that technology providers are often driving the use of technology by employers.⁴⁹ Two expert commentators, Johnston and Cheng, say:

48 A worker might use a drug on the weekend, but a random drug test on Monday morning might still reveal the presence of the drug in the worker's system. See VLRC (September 2004), above n 16, paras 2.72–92, for a discussion about the processes of drug and alcohol testing.

49 See, eg, consultations 9, 12 (Appendix 2 has the full list of consultations).

...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.⁵⁰

2.10 While the use of technology may be warranted in some circumstances, in other cases it may represent a disproportionate response to the risk which the employer is trying to manage. For example, an airline might be justified in conducting random alcohol and drug testing of its pilots for public safety reasons, but random testing of clerical and sales staff is more difficult to justify.

2.11 The potential for disproportionate uses of technology by employers is not only of concern to workers, but also to the wider community. In a survey commissioned by the federal Privacy Commissioner on community attitudes to privacy, 59% of respondents thought that an employer should only be permitted to conduct random drug testing if this was necessary to ensure safety.⁵¹ Approximately one-third of survey respondents did not support employers' use of surveillance equipment⁵² or reading of workers' emails.⁵³ About 40% only supported these practices when an employer suspected wrong doing.⁵⁴ In the commission's view, practices which affect workers' privacy can only be justified where the employers' actions are taken to protect a defined interest which outweighs workers' privacy rights, and where the action is proportionate to the interest the employer is seeking to protect.

LACK OF CERTAINTY

LEGISLATIVE GUIDANCE

2.12 While rapid developments in technology have given employers greater capacity to monitor their workers, they have not been accompanied by the development of

50 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.

51 See Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004) 57.

52 Ibid 53.

53 Ibid 52.

54 Ibid 52–3.

appropriate guidelines about the circumstances in which such monitoring should occur. In early consultations, some employers told us that guidance on these issues would be welcome. They also commented that existing legislation contains prohibitions on practices, without providing guidelines as to how these practices might be appropriately used. An example cited was the *Surveillance Devices Act 1989* (Vic) which sets out how surveillance measures must not be used,⁵⁵ but does not provide guidance on how they can be lawfully applied.⁵⁶ It was also said that assistance on how to implement and interpret drug-testing procedures would be helpful.

INCONSISTENT STATE AND FEDERAL LAWS

2.13 Some employer representatives were concerned about the development of a patchwork of overlapping and inconsistent privacy legislation.⁵⁷ They preferred a uniform national approach,⁵⁸ particularly businesses with national operations (such as banks). Others argued that current legislation ‘covered the field’ and that reform was not strictly necessary.⁵⁹

2.14 If guidance is needed, the preferred approach of some employer representatives is to have self-regulation. The self-regulatory measures proposed focused on enhanced education and practical guidelines.⁶⁰ Some support existed for the development of national guidelines,⁶¹ perhaps administered through the federal Privacy Commissioner.⁶² One employer representative described this approach as a ‘guided self-regulatory model’.⁶³

2.15 While acknowledging that national regulation would alleviate issues of inconsistency (and any related compliance costs), the commission does not believe that the states should avoid legislating to protect workers for this reason alone, especially

55 See, eg, *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1).

56 Consultation 5.

57 Options Paper submissions 11, 13, 22, 27. (See Appendix 3 for a full list of Options Paper submissions.) The issue of national consistency has also been raised in relation to the operation of information privacy laws. See Australian Government, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) ch 2.

58 Options Paper submissions 2, 11, 12, 22, 27.

59 Options Paper submission 24.

60 Roundtable 3 (Appendix 1 has the full list of roundtables).

61 Options Paper submissions 11, 27.

62 Options Paper submission 11.

63 Roundtable 4.

where no protection would otherwise exist. The NSW Law Reform Commission adopted this position in its interim report into surveillance, stating in relation to internet monitoring:

The Commission acknowledges that this two-tier system of regulation is not ideal...However, the law as it currently stands does not provide sufficient protection against privacy threats presented by the Internet. The Commission is of the view that it is better to sacrifice some clarity for the sake of comprehensive regulation.⁶⁴

2.16 Even assuming that the Commonwealth Government is able to exercise its constitutional power to 'cover the field' of workplace privacy, it may not be willing to do so. For example, the Commonwealth Government might conclude its current review of the employee records exemption by saying that no changes are to be made to the exemption (see paras 1.18–1.19 for detail on exemption). States might then wish to consider whether to legislate to protect employee records.

GAPS IN LEGAL PROTECTION

2.17 The commission has concluded that the existing legal regimes that regulate workers' privacy in Victoria offer piecemeal privacy protection at best and in some cases, such as physical and psychological testing, provide virtually no protection at all. These gaps were described in detail in the Options Paper and are reviewed briefly below.

SURVEILLANCE AND MONITORING LAWS

2.18 The use of surveillance devices by employers is regulated by the Surveillance Devices Act. Surveillance devices include video surveillance (the most common form of which is CCTV), audio surveillance (eg using a recorder to tape a conversation) and tracking devices (eg the use of GPS monitoring, which is common in the transport industry).

2.19 There are gaps in the way the Act regulates workplace surveillance. The most important gaps are:

- the Act may not cover all forms of surveillance or emerging technologies such as biometrics;

64 NSWLRC (2001), above n 1, 65.

- it will rarely apply to surveillance in the workplace because of the restricted definition of ‘private activities’ and ‘private conversations’;⁶⁵
- it offers no protection to workers who agree to employer use of surveillance devices in circumstances where they may not feel they are free to withhold their consent.⁶⁶

2.20 There has also been considerable uncertainty about whether employer monitoring of worker email and internet usage is regulated by existing legislation. These practices do not appear to be covered by the Act and there is also some uncertainty about whether the federal Telecommunications (Interception) Act regulates employer monitoring of emails and other types of messages such as voicemails and SMS. Thus, it is unclear whether these kinds of communications would be considered to be the interception of a communication ‘passing over a telecommunications system’,⁶⁷ and hence prohibited under section 7(1) of the Telecommunications Interception Act. The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) now expressly excludes ‘stored communications’, such as emails, from the current prohibition against interception of

65 A ‘private activity’ is one carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include (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 it may be observed by someone else: see *Surveillance Devices Act 1999* (Vic) s 3. A ‘private conversation’ is one carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it may be overheard by someone else: see *Surveillance Devices Act 1999* (Vic) s 3.

66 See paras 2.23–2.24 on ‘worker consent’.

67 The technology of emails is such that, as between the sender and intended receiver of an email, the message may ‘sit’ for a period, or even indefinitely, on a network or internet service provider’s server. If ‘passing over’ is considered to be all the stages between sending and receipt of the message (including all intermediate points at which storage may occur), then accessing and monitoring of email while it is ‘sitting’ on a server may be an ‘interception’. If, however, ‘passing over’ were to be interpreted as limited to the actual transmission of the message over the cables or optic fibres, then the accessing of an email when it is sitting on the server would not be an interception. There is another point of doubt with respect to emails, which arises from 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 that is not part of the carrier’s telecommunications network or whether it is a telecommunications network in its own right, separate from that of the carrier. If it is a separate network made up of a number of computers with communications passing between them ‘by means of guided or unguided electromagnetic energy or both’ (*Telecommunications (Interception) Act 1979* (Cth) s 5), then the accessing and monitoring of emails in the workplace may be subject to the Act (although subject to the same exclusion with respect to stored communications).

communications under section 7(1).⁶⁸ The exclusion will operate for 12 months from December 2004, while the government undertakes a comprehensive review of Australia's interception regime.⁶⁹ What the recommendation of this review will be is presently unknown, as is the extent of future federal regulation in this area.

TESTING LAWS

2.21 Existing privacy legislation does not explicitly regulate workplace testing, though it places some limits on collection of information by testing and on the use or disclosure of that information. For example, any 'health information' collected from the process of medical testing would be governed by the provisions of the Health Records Act.⁷⁰

WORKPLACE LAWS

2.22 Other laws that are relevant to the workplace offer no direct privacy protections. Privacy is not an 'allowable award matter' and so cannot be the subject of federal award regulation (see section 89A of the Workplace Relations Act).⁷¹ Similarly,

68 The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) became effective in December 2004. Its aim is to exclude 'stored communications' from the prohibition against interception in the Telecommunications (Interception) Act. The Act defines a 'stored communication' as one which is stored on equipment or any other thing: sch 1, s 4. According to the Explanatory Memorandum, the amendments will have the effect of limiting the prohibition against interception to the 'real time' interception of communications transiting a telecommunications system. The rationale behind these amendments was explained as ensuring 'that the interception regime keep pace with technological developments' where the Telecommunications Interception Act was proving difficult to apply 'to modern telecommunications services...such as voicemail, email and SMS messaging'—see the Second Reading Speech, Commonwealth Parliamentary Debates, House of Representatives, 27 May 2004 (Phillip Ruddock, Attorney General) 29311.

69 Ibid 29130. The commission is informed by the federal Attorney-General's office that the 12 month review period 'sunset' on 15 December 2005. A report containing recommendations to the federal government has been prepared, but at the time of writing had not yet been publicly released. It was indicated that the federal government would have to take legislative action between the time the report was released and 15 December 2005 (National Security and Criminal Justice Division—Attorney-General's Department [Cth] 25 August 2005).

70 The *Health Records Act 2001* (Vic) contains 11 Health Privacy Principles which regulate matters such as the collection, use, disclosure, storage and security of health information.

71 Certified agreements are not restricted to allowable award matters and may deal with privacy issues that pertain to the employment relationship. But so far, certified agreements have been infrequently used to deal with workplace privacy issues—perhaps with the exception of drug and alcohol testing procedures—and workers may be unable to obtain an employer's agreement to the inclusion of clauses protecting privacy in Australian Workplace Agreements and in contracts of employment, because of their lack of bargaining

the Equal Opportunity Act and the Occupational Health and Safety Act protect workers who have experienced discrimination or a threat to their health and safety, but are not primarily concerned with privacy. The remedies provided under these laws are generally only available where the worker has suffered some specific form of detriment such as discrimination, loss of employment or pay, or a demotion. It is unlikely that these remedies will provide relief for workers who have 'only' suffered damage to their sense of autonomy and dignity.

CONSENT AND INVASIONS OF WORKPLACE PRIVACY

2.23 Consent plays a central role in labour law as well as in aspects of privacy and surveillance law. By 'consent' we mean 'a voluntary agreement, the act or result of coming into accord. It is an act that is unclouded by fraud or duress'.⁷² 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'.⁷³ Individual workers often have little real power to object to practices that affect their privacy. They may be required to agree to such practices to obtain or keep a job. Their consent may not be voluntary in the sense of a consent given freely without fear of reprisal by the employer. Current remedies for invasions of privacy do not apply when workers have consented to the practices involved.

2.24 In the collective bargaining process, the consent of a representative body such as a union may be more meaningful than individual worker consent since the power imbalance between unions and employers is not as great. However, a high percentage of the workplace is non-unionised. The Australian Bureau of Statistics puts trade union membership in 2004 at 22.7% of the surveyed labour force.⁷⁴ Nor do unions specifically represent non-employees such as job applicants, independent contractors and volunteers.

power. While there is the potential for an exceptional matters order pursuant to section 89A(7) of the Workplace Relations Act, few orders have been issued in practice.

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

73 Caroline Morris, 'Drugs, the Law, and Technology: Posing Some Problems in the Workplace' (2002) 20 *New Zealand Universities Law Review* 1, 27.

74 Australian Bureau of Statistics, *Employee Earnings, Benefits and Trade Union Membership*, Catalogue 6310.0 (2004) 39.

OTHER JURISDICTIONS

2.25 The importance of workplace privacy has been recognised by a number of overseas bodies.⁷⁵ These include the International Labour Organization,⁷⁶ the Council of Europe⁷⁷ and the European Commission.⁷⁸

2.26 The European Commission is considering strengthening protection for workers' privacy through the introduction of a directive specifically concerned with the protection of workers' data.⁷⁹ This would build on the existing European Union data protection directive by formulating measures on how data protection should apply in the workplace context.⁸⁰ The European Commission has also considered the surveillance of electronic communications in the workplace.⁸¹

2.27 Although workplace privacy regulation in Europe is generally piecemeal,⁸² Finland has introduced comprehensive workplace privacy legislation in the form of one Act that regulates drug testing, personality and aptitude tests, genetic testing, surveillance and email monitoring, as well as protecting employee data.⁸³ The Finnish

75 The regulation of workplace privacy in other jurisdictions is discussed in Issues Paper submission 29. (Appendix 4 has the full list of Issues Paper submissions.)

76 See, eg, International Labour Office, *Protection of Workers' Personal Data: An ILO Code of Practice* (1997); International Labour Office, *Management of Alcohol- and Drug-Related Issues in the Workplace*, An ILO Code of Practice (1996).

77 See Council of Europe, Committee of Ministers, *Recommendation No R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment Purposes*, 423rd meeting of the Ministers' Deputies (entered into force 18 January 1989).

78 See, eg, European Commission Article 29 —Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (2001); European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (2002); European Commission Article 29 —Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace* (2002).

79 European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (2002).

80 Issues Paper submission 29.

81 European Commission Article 29 —Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace* (2002).

82 Issues Paper submission 29.

83 See translation of the *Act on Protection of Privacy in Working Life* (759/2004), *Data Protection in Working Life*, Ministry of Labour, <www.mol.fi/mol/en/03_labourlegislation/03_privacy/index.jsp> at 24 May 2005.

Act was pointed to by some unions in our consultations as being a desirable model for workplace privacy regulation, particularly in relation to drug testing.⁸⁴

2.28 A number of national privacy and data protection commissioners have turned their attention to workplace privacy issues.⁸⁵ For example, in the United Kingdom the Information Commissioner has issued a code for employers that sets out good-practice recommendations on conducting workplace surveillance and monitoring and handling employee records (including health information).⁸⁶ Any enforcement action would be based on an employer's failure to meet the requirements of the *Data Protection Act 1998* (UK), which protects the personal data of individuals, including workers. If there is an action alleging breach of the Act, relevant parts of the code are likely to be cited by the commissioner.⁸⁷ In Hong Kong, the Office of the Privacy Commissioner has released codes and guidelines on workplace privacy issues.⁸⁸ These issues have also received attention from the Information and Privacy Commissioner in Ontario.⁸⁹

2.29 Workplace privacy protections in the United States variously arise under common law governing employment relationships,⁹⁰ tort law,⁹¹ in collective

84 Roundtable 2. See translation of the *Act on Protection of Privacy in Working Life* (759/2004) sections 6–12, *Data Protection in Working Life*, Ministry of Labour, <www.mol.fi/mol/en/03_labourlegislation/03_privacy/index.jsp> at 24 May 2005. In summary, these provisions provide that the employer is limited to processing information from a test of an employee's drug use which is contained in a drug test certificate supplied to the employer by the person concerned. A drug test certificate is issued by a health care professional and laboratory designated by the employer. An employer may require an employee to present a drug test certificate if the employer has 'justifiable cause to suspect that the employee is under the influence of drugs at work', and only if testing is essential to establish functional capacity. The type of work must require precision, reliability, independent judgment or quick reactions and must be capable of resulting in a specified form of endangerment/breach of public interest. Similar provisions exist in the recruitment context, though there is no 'justifiable cause' requirement. Instead, an employer can only process information from a drug certificate with the consent from the applicant who has been successfully selected for the job.

85 Issues Paper submission 29.

86 Information Commissioner's Office [UK], *Data Protection: The Employment Practices Code* (June 2005).

87 Ibid 4.

88 See Office of the Privacy Commissioner for Personal Data, Hong Kong, *Code of Practice on Human Resource Management* (2000).

89 See, eg, Information and Privacy Commissioner, Ontario, *Workplace Privacy: A Consultation Paper* (1992); Information and Privacy Commissioner, Ontario, *Workplace Privacy: The Need for a Safety-Net* (1993); Information and Privacy Commissioner, Ontario, *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office* (2001).

90 John Craig, *Privacy and Employment Law* (1999) 59–61, see 'Employment-at-will Doctrine'. See also Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (2003) 116,125–6, 128–131.

agreements⁹² and in public sector information privacy legislation.⁹³ The federal *Bill of Rights* and 11 state constitutions confer privacy protection on citizens⁹⁴ and an array of statutory provisions exists at both federal⁹⁵ and state levels.⁹⁶ Statutory protection afforded employees in the United States ‘varies markedly from state to state’⁹⁷ and covers practices as diverse as HIV testing, polygraphs and employer control of off-duty activities.⁹⁸

2.30 Workplace privacy is also being considered in other Australian jurisdictions. The New South Wales Government has recently passed an Act to extend the scope of its workplace video surveillance legislation to regulate other forms of workplace surveillance.⁹⁹ The Act includes the regulation of workplace email and internet monitoring.¹⁰⁰ It also distinguishes between the surveillance that an employer can carry

91 Craig, *ibid* 71, 73; see tort of wrongful discharge in contravention of public policy and tort of invasion of privacy.

92 *Ibid* 61, see para 4.3.3.

93 *Ibid* 61, 69, 70.

94 *Ibid* 61, see para 4.3.3.1.

95 *Ibid* 81–84. See also Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (2003) 120.

96 Craig, *ibid* 80, see para 4.3.4.4 for examples of statutory provisions.

97 *Ibid* 81.

98 *Ibid* 80–81.

99 The New South Wales Government has enacted the *Workplace Surveillance Act 2005*. The commission was informed by the Legislation and Policy Division of the NSW Attorney-General’s Office (31 August 2005) that the date of commencement is 7 October 2005. According to the Explanatory Note to the Workplace Surveillance 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 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. It applies to camera surveillance, computer surveillance and tracking surveillance (surveillance of the location or movement of an employee). The Act is intended to replace the existing *Workplace Video Surveillance Act 1998* (NSW) which applies only to video (ie camera) surveillance.

100 *Workplace Surveillance Act 2005* (NSW) s 17 prohibits the blocking of emails sent to or by an employee and internet access by an employee. This is unless the employer is acting in accordance with the employer’s email and internet access policy which has been notified in advance to the employee and (except in the case of spam or menacing, harassing or offensive emails) the employee is notified as soon as practicable that an email has been blocked. An employer’s email and internet access policy cannot authorise blocking of emails and internet access merely because the content relates to industrial matters. See also Explanatory Note to the Bill, 3.

out when an employee is at work and when the employee is not at work.¹⁰¹ It has been reported that the Queensland Government is considering introducing legislation on the regulation of workplace email and internet monitoring.¹⁰² We have also been informed that attempts were made to amend South Australian industrial relations legislation to include provisions on workplace surveillance, but these proposed amendments were not enacted.¹⁰³

CONCLUSION

2.31 The impetus for the protection of workers' privacy is growing, both in Australia and overseas. Given our recognition of privacy as a fundamental human right, the commission believes that if the right is to be adequately protected in Victorian workplaces, there is a need to reform our existing laws. The need for reform arises from:

- the rapid advances in technology that have occurred and are continuing to occur;
- the difficulties in obtaining meaningful worker consent to any testing and surveillance practices that are used or proposed to be used;
- the current gaps in legislative protection;
- the lack of mechanisms to balance the interests of workers and employers.

101 *Workplace Surveillance Act 2005* (NSW) s 16 prohibits the surveillance by an employer of an employee by means of a work surveillance device when the employee is not at work, except by means of computer surveillance of the employee's use of employer provided equipment or resources. Section 3 of the Act defines computer surveillance as surveillance by means of software or other equipment that monitors or records information input or output, or other use of a computer (including the receipt and sending of emails and internet access).

102 Joanna Musk, 'Workplace rules set to widen', *Privacy Update* (April 2005), <www.minterellison.com> at 2 June 2005. The commission was informed by Strategic Policy Branch in the Queensland Department of Justice and the Attorney-General's office (19 July 2005) that proposed workplace surveillance laws will be looked at possibly later in 2005.

103 The commission was informed of this by Policy and Strategy Group, Workplace Services, Department of Administrative and Information Services, South Australia (19 July 2005). See also South Australia, *Parliamentary Debates*, House of Assembly, 9 March 2005, 1998–1999 (Mr Hanna); South Australia, *Parliamentary Debates*, Legislative Council, 1 March 2005, 1232–34, 1242–43.

FEEDBACK ON THE OPTIONS

2.32 How is law reform to be effected in this area? What is the most appropriate form of regulation?

2.33 The commission considered a number of regulatory options in the Options Paper, including self-regulatory options such as best practice guidelines and education, incentive-based schemes and reputation-based sanctions. The commission concluded that none of these options were able to guarantee an appropriate balance of the interests of employers and workers' privacy. However, some aspects of these models were considered useful when combined with other enforcement techniques. With these objectives in mind, the commission proposed two options to regulate workplace surveillance, monitoring and testing practices:

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.

2.34 Following the publication of the Options Paper, the commission organised roundtable consultations with employers, employer organisations, unions, regulators, lawyers and academics about the proposed options. It also received a number of written submissions. From the comments made in roundtables and submissions it became apparent that neither Option 1 nor Option 2 would be appropriate to regulate all types of surveillance, monitoring or testing practices that had been identified in our investigations. Responses from a number of participants pointed towards a regulatory approach combining elements of Options 1 and 2. We describe below some of the responses received on the options and then outline the model that the commission now proposes for adoption.

AUTHORISATION NOT APPROPRIATE FOR ALL PRACTICES

2.35 We received considerable feedback on the 'authorisation model' set out in Option 1. Most parties did not favour an authorisation model. The principal reasons advanced against this option were resource allocation and compliance costs, undue interference with management prerogatives and perceived inconsistencies with other relevant regulatory frameworks. These matters are considered briefly below.

RESOURCE ALLOCATION AND COMPLIANCE COSTS

2.36 Employers were concerned about compliance costs caused by undue bureaucratic requirements, inefficiency and delay.¹⁰⁴ For example, they were worried that waiting for an authorisation for covert monitoring and/or surveillance could lead to a loss of evidence needed to substantiate allegations that an employee was involved in illegal activities.¹⁰⁵ There was also concern that if the authorisation regime was too complicated employers would need to obtain legal advice before seeking an exemption and/or an authorisation, which would add to the delay and cost involved.¹⁰⁶ A technology provider indicated that requiring employers to seek authorisation was likely to lead to a reduction in the availability of online privileges to workers.¹⁰⁷

2.37 While it was thought that larger employers might potentially be better placed to deal with the authorisation process, it was argued that it would be disproportionately difficult and costly for small employers,¹⁰⁸ leading to the risk that they might put a practice in place without bothering with an authorisation.¹⁰⁹ An employer organisation mainly representing small business referred to current levels of business regulation which small business found difficult to comply with.¹¹⁰ It was argued that the proposed authorisation model would add to these complications.¹¹¹

2.38 In the Options Paper, the commission suggested industry-wide authorisations could alleviate some of the cost and resource allocation issues. However, this aspect of the model received little support from either unions or employers.¹¹²

2.39 Concerns were also raised as to whether the government was likely to provide the regulator with the necessary resources to enable the authorisation system to operate effectively,¹¹³ including the costs associated with educating employers and workers about any new system.¹¹⁴ One view was that this option would not be implemented in

104 Options Paper submissions 12, 15.

105 Roundtable 5.

106 Roundtable 5.

107 Options Paper submission 8.

108 Options Paper submission 22.

109 Roundtable 5.

110 Roundtable 3.

111 Roundtable 3.

112 Roundtables 2, 3; Options Paper submissions 4, 9, 18, 22, 23, 24, 30.

113 Roundtables 1, 2.

114 Options Paper submission 12.

its entirety given the government's resource constraints,¹¹⁵ while others felt the potential cost could have a significant impact on the viability of the model.¹¹⁶ In the absence of appropriate resources and support, the authorisation model could become a 'tick-a-box' process—a 'toothless tiger'—and as such ignored.¹¹⁷

UNDUE INTERFERENCE WITH MANAGEMENT PREROGATIVE

2.40 Employers were concerned about a third-party regulator making decisions that would affect their businesses.¹¹⁸ Some roundtable participants had reservations about the expertise or background of a proposed regulator¹¹⁹ and the regulator's ability to understand the nature of specific industries.¹²⁰ One employer organisation asserted that the capacity of a regulator to make judgments about the reasonableness of an employer practice was inconsistent with the notion that an employer has the right to run its business effectively.¹²¹

MARKET FAILURE

2.41 A small number of employer representatives raised the argument that regulation of practices is not required except where an identifiable market failure has occurred.¹²² This argument suggested that the 'market' is capable of producing required levels of protection for workers as a result of supply and demand and the competition generated within the job market. For instance, if a business wished to attract highly skilled software engineers, favourable employment conditions would contribute to the employer's competitive edge. Accordingly, where unsavoury workplace privacy practices detract from the attractiveness of the business, the employer would modify or dispense with such practices. However, this logic does not apply as easily to types of work that are not in demand or highly specialised. For

115 Roundtable 4.

116 Roundtable 5.

117 Roundtable 4.

118 Roundtable 5; Options Paper submission 24.

119 Roundtable 2.

120 Options Paper submission 15.

121 Options Paper submission 11. The submission referred to this as a 'Privacy Act concept'. Presumably, by Privacy Act concept the submission is referring to one of three general objects contained in the *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3, that 'recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently'.

122 Options Paper submissions 11, 12.

instance, assembly-line workers are unlikely to ‘vote with their feet’ and find alternative employment in another privacy-friendly business, particularly when jobs are scarce. Similar constraints apply within an ongoing work relationship.

2.42 It is also difficult to see how market regulation would stem any proliferation of potentially privacy-invasive technologies as availability is driven by employer demand. For this reason, a roundtable participant did not think the wait-and-see approach involved in gauging market failure was appropriate, instead seeing regulation as necessary to control the use of new technologies.¹²³ The interplay of market forces does not ‘correct’ uses of technologies, imbalances of power and inequalities in demand, and results in different levels of protections for different workers. This makes it inappropriate to rely on market failure to provide appropriate regulation.

INCONSISTENT POLICY APPROACH

2.43 Some roundtable participants referred to the federal government’s policy agenda to deregulate workplace relations and suggested that the regulatory mood was for a less strict approach than would be involved in an authorisation process.¹²⁴ A regulator from a similar regulatory regime agreed with this, cautioning against a heavy hand in what was described as the ‘era of the light touch’.¹²⁵ It was also suggested that the current state government approach was to develop framework legislation and then provide codes of practice (such as in the areas of outworker and child employment protection).¹²⁶

2.44 Some parties also commented on the possibility of complex overlaps with other laws such as those relating to occupational health and safety.¹²⁷ One employer argued that the model contradicted the principal objectives of the federal Workplace Relations Act, which placed primary responsibility for determining matters affecting the employer–employee relationship at the enterprise level.¹²⁸ Concerns were also raised about the limitations of state legislation, which could be overridden by federal industrial agreements.¹²⁹ A union stated that where the authorisation model did not

123 Roundtable 4.

124 Roundtable 3.

125 Roundtable 1.

126 Roundtable 2.

127 Roundtable 1.

128 Options Paper submission 12.

129 Roundtable 1.

provide at least equivalent protection to workers as that available in certified agreements, the 'retrograde' result would be lower levels of privacy protections for those workers who fell outside the certified agreement system.¹³⁰

AUTHORISATION APPROPRIATE FOR VERY INTRUSIVE PRACTICES

2.45 From the responses referred to above, it is apparent to the commission that a regime requiring authorisation of all surveillance, monitoring and testing practices would be a disproportionate regulatory response. Such a regime would be likely to impose a significant cost and resource burden on employers, particularly on small business. Our proposed model therefore does not require authorisation of all potentially privacy-invasive practices (see para 3.6–3.7).

2.46 Nonetheless, the commission considers that authorisation is an appropriate response in certain limited and clearly defined instances, namely those involving very intrusive practices that may have serious consequences for workers. This is because an authorisation model is a proactive form of regulation that aims to prevent privacy breaches before they occur. It places the onus on the employer to show why workers' privacy should be breached in such cases by requiring them to justify the proposed practice.¹³¹ It also elevates workplace privacy as an issue¹³² and circumvents the need for reliance on workers' consent to practices, which is often problematic in the workplace context. An authorisation has the added benefit of providing certainty to employers and workers by clearly setting out what an employer can and cannot do in relation to implementing the practice in question.¹³³

2.47 The approach taken in limiting the use of authorisation to privacy-intrusive practices also accords with the state government's *Victorian Guide to Regulation*, which encourages regulatory measures to be the minimum necessary to achieve desired objectives. The commission has taken into account the guide's principles in developing its regulatory model.

2.48 In Chapter 4, we describe the way in which authorisation could be incorporated into the proposed regulatory model and outline the particular practices where we believe authorisation is appropriate.

130 Roundtable 2.

131 Roundtables 1, 2.

132 Roundtable 2.

133 Roundtables 1, 2, 3, 5; Options Paper submission 4.

PRINCIPLES AND CODES APPROPRIATE FOR MOST PRACTICES

2.49 Employers and employer representatives were generally more in favour of principles and codes than a prescriptive regulatory option. Some employers and employer organisations believed that general principles would give them flexibility to interpret the law to adapt to their workplace and existing legal obligations.¹³⁴ They also liked the idea of practical codes of practice to accompany the principles.¹³⁵

2.50 One concern raised by some parties was that principles-based regulation might, in practice, offer little real privacy protection to workers.¹³⁶ There was apprehension that general principles would be difficult for employers to comply with¹³⁷ and that this could encourage a regime of ‘paper compliance’, where employers merely pay lip service to principles rather than genuinely complying with them. A number of parties also thought that the enforcement provisions in Option 2 required strengthening. One roundtable participant suggested that Option 2 should incorporate an audit and investigative function.¹³⁸ Another proposed that principles be accompanied by a general duty to respect privacy¹³⁹ that could be supplemented by codes of practice. Compliance with such codes could be used as a defence to a claim that an employer breached its duty. It was also suggested that if a general duty were used, then the right to privacy would need to be defined.¹⁴⁰

2.51 The commission accepts the force of the arguments in favour of principles and codes. There are advantages in having a regime that is flexible enough to take account of varying workplace requirements. The issue of uncertainty arising from having general principles could be, to some extent, overcome by detailed codes on particular practices or by industry codes.¹⁴¹ The commission was impressed by the general level of support for this approach, as articulated by parties in their submissions and roundtable discussions.

134 Roundtables 2, 4, 5; Options Paper submissions 2, 8, 12, 15, 20, 24.

135 Roundtable 5.

136 Roundtable 5.

137 Roundtables 1, 3.

138 Roundtable 1.

139 Roundtable 1.

140 Roundtable 2.

141 There was some support for industry specific codes, although one employer thought that these might be difficult for multi-industry companies to comply with: roundtables 1, 4.

2.52 However, while principles and codes may be acceptable for many practices, the commission does not support them in all cases. It is apparent from the roundtables and submissions that parties view some practices as more intrusive than others. The varying levels of potential intrusiveness that exist suggest that the best regulatory model is one that encompasses different kinds of regulation for different practices. Such a 'hybrid' approach, that is a combination of different types of regulation, was also suggested by a number of participants.¹⁴²

HYBRID MODEL

2.53 The comments on the two options received in submissions and during roundtables highlighted to the commission the complexity of the issues involved in proposing appropriate regulatory models for workplace privacy. After considering the matters, together with the comments of interested parties, the commission has decided to recommend a tiered regulatory regime that combines a number of mechanisms. These are described in the next chapter.

142 See, eg, Options Paper submissions 5, 14, 23, 28, 31; roundtables 1, 2.

Chapter 3

Balancing Employer and Worker Interests

INTRODUCTION

3.1 Chapter 2 has made the case for reform of laws affecting workplace privacy. Privacy is recognised as a basic human right in international conventions to which Australia is a signatory.¹⁴³ Promotion and protection of human rights is also one of the Victorian Government's primary strategic aims.¹⁴⁴ People do not expect to forfeit all protection of their privacy simply because they are working. Rapid advances in technology now allow employers to scrutinise the activities of workers and have access to details of their private lives, to an extent that was impossible in the past.

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

143 Chapter 2, paras 2.2–2.3.

144 See Department of Justice [Victoria], *Department of Justice Strategic Priorities 2005: A Framework for Planning and Opportunities for Collaboration* (2005) <www.justice.vic.gov.au> at 5 September 2005, which includes in its top six priorities 'Justice Statement Implementation' which contains a 'major project on human rights'; Department of Treasury and Finance, *Victorian Guide to Regulation* (2005) 5-4 <www.vcec.vic.gov.au> at 5 September 2005, which asks whether the objectives of regulation are 'consistent with Government's strategic aims'. At 2-2 the guide specifically refers to 'addressing social welfare objectives' where 'in addition to addressing market failure, government intervention can be justified in the pursuit of social and equity objectives'. This includes social policies such as 'human rights, protecting the vulnerable and disadvantaged'.

3.3 A number of factors must be considered in deciding whether an act or practice undertaken by an employer unreasonably breaches a worker's privacy, including the extent of the privacy invasion, the reasons for the act or practice and the workplace context in which it has occurred. For example, it may be reasonable for an employer to require workers doing dangerous work to be regularly tested for alcohol use, but unreasonable for an employer to require a clerical worker to undergo similar tests. Laws which regulate workplace privacy must be able to provide flexible responses which take account of the problems which arise in particular workplaces, while at the same time providing consistency and certainty for both workers and employers. They must also be responsive to developments in technology which have the potential to affect privacy and changes in social attitudes about the use of these technologies.

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

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

REGULATORY FRAMEWORK

3.5 In Chapter 2 we explained our reasons for recommending a regulatory scheme which combines several elements. As mentioned, in developing our proposed scheme we have also taken into account the recommendations contained in the *Victorian Guide to Regulation*.¹⁴⁵

145 Department of Treasury and Finance (2005), above n 144.

LIGHT-TOUCH REGULATION WHERE POSSIBLE

3.6 Regulation which is not intrusive or prescriptive and is cheap to administer and comply with is often described as ‘light touch’.¹⁴⁶ The employers we consulted tended to favour a light-touch regulatory approach. In the context of workplace privacy, light-touch regulation would emphasise the importance of educating employers about privacy protection. It would impose a general obligation on employers to avoid unreasonably breaching the workers’ privacy, rather than setting out detailed rules as to how this should be done. It might also include non-binding codes to assist employers in deciding which practices were in keeping with their broad obligations. Such an approach is consistent with that adopted in the *Victorian Guide to Regulation* which advocates, where possible, the minimum regulatory measures necessary to achieve the desired objectives.¹⁴⁷

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

STRICTER CONTROLS FOR SERIOUS PRIVACY INTRUSIONS

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

146 National Economic Research Associates, *Alternative Approaches to ‘Light-Handed’ Regulation: A Report for the Essential Services Commission Victoria* (2004) 8.

147 Department of Treasury and Finance (2005), above n 144, 3-3.

regulation¹⁴⁸ and was also supported in a number of employee and employer submissions. The Victorian Trades Hall Council describes this as, 'a hierarchy of intrusions some of which require far more stringent testing than others...'.¹⁴⁹

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

if a regulatory system requiring authorisation is implemented, clearly it should be a limited system with only the most intrusive workplace surveillance, monitoring and testing requiring authorisation.¹⁵⁰

3.10 This acknowledges the fact that the level of intrusion will vary, depending on the practice and the context. The commission's approach is to ensure the level of regulation matches or corresponds to the level of intrusion.¹⁵¹ This regulatory approach combines performance-based regulation with more prescriptive measures.

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

SUMMARY OF PROPOSALS

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

- Light-touch regulation will apply to most practices which affect workers when they are involved in work-related activities. The legislation imposes an obligation on employers not to unreasonably breach the privacy of workers while they are working. The regulator will have power to issue advisory codes of practice to provide guidance on this obligation or to approve codes

148 Ibid 2-2, which classifies 'social policies' as including 'human rights, protecting the vulnerable and disadvantaged'.

149 Options Paper submission 28.

150 Options Paper submission 22.

151 This is consistent with Department of Treasury and Finance (2005), above n 144, 3-87, which refers to 'performance-based regulation' as specifying 'desired outcomes or objectives, but not the means by which these outcomes/objectives have to be met' in contrast to prescriptive regulation requirements which set out in detail specified, objective criteria and standardised solutions.

developed by employers. The codes may indicate how employers should undertake particular activities (eg surveillance in open areas in the workplace) or monitoring email and internet use over an employer-provided communication system. If a worker complains about a privacy invasion, the complaint will not be upheld if the employer has followed an advisory code of practice. Failure to comply with an approved code will be a breach of the employer's obligation not to unreasonably breach the privacy of workers.

- The regulator will be required to produce codes of practice (mandatory codes) to govern activities affecting workers which are particularly privacy invasive. These include covert surveillance of workers while they are working and taking bodily samples from workers to test for the presence of drugs and alcohol. Failure to comply with a mandatory code will be a breach of the employers' obligation not to unreasonably breach workers' privacy.
- Some practices which affect privacy will require authorisation in advance by the regulator. Authorisation will be required if the practice affects a person while they are not working, for example out-of-hours surveillance of a worker who is suspected of theft. We argue that genetic testing is particularly privacy intrusive and should also require authorisation by the regulator. The legislation will allow authorisation requirements to be extended to new technologies which have a significant impact on workers' privacy.
- Surveillance in private areas in the workplace, for example in toilets and bathrooms, will be prohibited. These are areas in which all members of the community have a very high expectation of privacy. Placing workers under surveillance in these areas would have an unacceptable effect on their human dignity and autonomy.

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

WORK-RELATED AND NON-WORK-RELATED ACTIVITIES

3.14 As we explained above, the recommended legislation generally gives workers greater privacy protection outside the work context than the privacy protection they will receive when they are working. It will therefore differentiate between the controls imposed on employer practices which affect workers involved in work-related as

opposed to non-work-related activities. This distinction reflects the differing balance between employers' interests and workers' expectations of privacy in these two contexts.

3.15 We have used the term 'activities', qualified by the adjectives 'work' and 'non-work', because, while the workplace may be a relevant distinguishing factor in many instances, it is not determinative of whether or not work is being performed. Relating the performance of work to activities is more precise than attempting to locate a physical workplace, and more accurately reflects the nature of and liabilities arising from the modern work relationship (see Chapter 1 para 1.31–1.32 for discussion on the breadth of the modern workplace).

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

3.17 Although workers may expect a lower level of privacy at work than in other aspects of their lives, they do not leave their right to privacy at the door.¹⁵² Whether a particular practice achieves a fair balance between workers' reasonable expectations of privacy and employers' interests depends on both the purpose for which a particular act is being done and the nature and extent of the privacy invasion. For example, employers may wish to use overt video surveillance in some parts of the workplace to reduce stock theft. Installation of video cameras in toilet cubicles could reduce the possibility of theft even further, but most employers and workers would regard this as an unjustifiable invasion of workers' autonomy and dignity. We recommend employers should have a legislative obligation not to unreasonably breach the privacy of a worker while the worker is engaged in work-related activities. The concept of 'reasonableness' allows a range of factors to be taken into account in balancing employers' legitimate interests and workers' privacy. The content of this duty will be clarified in legislative principles.

3.18 When workers' conduct occurs outside work, it is much harder to argue that the employer has a legitimate interest in their activities. The employer does not have

152 VLRC (September 2004), above n 16, para 3.54.

an 'unfettered right to sit in judgement of out of work behaviour'.¹⁵³ Most people expect to be left alone by their employers when they are engaged in non-work-related activities. This expectation of privacy should attract a higher standard of protection than the privacy protection to which workers are entitled when they are at work. The fundamental social value underpinning this expectation can be summed up in a comment made at one of our roundtables that a person can never be someone else's property.¹⁵⁴ This is reflected in the NSW Workplace Surveillance Act, which prohibits surveillance when the employee is not at work.¹⁵⁵

3.19 The commission's Occasional Paper *Defining Privacy* argued that there is a public interest in recognising the privacy of all members of society, regardless of whether they are workers.¹⁵⁶ This public interest is upheld by protecting the privacy of workers outside the work context. The distinction which the proposed legislation makes between privacy protection inside and outside work is consistent with employment law. An employer's ability to discipline workers for their after-hours conduct is limited to activities with a direct link to their employment and which have a serious and significant impact on the workplace or employer's interests.¹⁵⁷ Similarly, employer liability for discriminatory acts of employees diminishes as the conduct becomes increasingly remote from the work relationship.¹⁵⁸

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

153 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. See also *Rose v Telstra* (Unreported, AIRC, Vice-President Ross, 4 December 1998, Print Q9292) 19.

154 Roundtable 5.

155 *Workplace Surveillance Act 2005* (NSW) s 16. Note that this does not apply to computer surveillance, as defined in s 3.

156 Foord (2002), above n 13.

157 Mary-Jane Ierodiaconou, 'After Hours Conduct' (2004) 78 (4) *Law Institute Journal* 42, 42-45.

158 *Ibid*, for examples of anti-discrimination law cases.

3.21 The recently enacted NSW Workplace Surveillance Act does not rely on the distinction between work and non-work but rather distinguishes surveillance on the basis of whether it is conducted in an overt or covert manner. The commission does not adopt this distinction in our proposed legislation because the practices in our terms of reference are much broader than surveillance and the covert–overt distinction is of little relevance to a practice such as drug and alcohol testing. Consistent with the NSW approach, however, we have used the covert–overt distinction to regulate surveillance, imposing stricter controls on covert than overt forms of surveillance (explained in para 3.82–3.90).

3.22 Our proposed differentiation between practices which affect workers undertaking work-related and non-work-related activities makes it necessary to define these terms. Employers need guidance about when workers’ activities are work-related and when they are not because their obligations are based on this difference.

DEFINITION OF WORK-RELATED ACTIVITIES

3.23 The definition of work-related activities must take account of the characteristics of the modern workforce. Multiple, global, mobile and cyber workplaces are becoming increasingly common. Workers may do their work at the premises of the employer, in a number of different places outside these premises, or at home.¹⁵⁹ Employers’ health and safety obligations and their potential liability for discrimination and sexual harassment are not limited to situations when workers are on their premises—they also cover workers while they are working elsewhere.

3.24 The recommended definition of work-related activities is loosely based on the ‘at work’ definition contained in the NSW Workplace Surveillance Act.¹⁶⁰ Work-related activities include:

- activities of a worker done in the course of performing work for the employer at the premises of the employer, or at any place other than the worker’s home or residence;

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

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

- use of the employer's communication systems, wherever the worker is located.

The key terms in the definition are explained below.

PERFORMING WORK FOR THE EMPLOYER

3.25 Workers' compensation law imposes obligations on employers when employees are acting 'in the course of their employment'.¹⁶¹ Similarly, an employer can be liable for torts (civil wrongs) committed by employees in the course of their employment,¹⁶² and much of employment law¹⁶³ is structured around this concept. Because our proposed legislation will cover independent contractors and volunteers as well as employees, our proposed definition refers to the performance of work rather than employment. The provision will ensure that when workers are performing activities in the course of their work,¹⁶⁴ at the premises of the employer or elsewhere, acts or practices which affect privacy will generally be governed by the employer's obligation not to unreasonably affect the worker's privacy. As we discuss below, guidance on the content of this obligation will be provided by principles in the legislation and by advisory or mandatory codes issued by the regulator.

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

161 See *Accident Compensation Act 1985* (Vic) s 3, which states the objects to the Act are (a) to reduce the incidence of accidents and diseases in the workplace and (i) in this context, to improve the health and safety of persons at work and reduce the social and economic costs to the Victorian community of accident compensation. Section 4 states (1) Despite anything to the contrary in this Act (a) this Act, other than Divisions 6A and 6B of Part IV, applies to and in relation to an injury to a worker on or after the appointed day arising out of or in the course of employment on or after the appointed day.

162 See John Fleming, *The Law of Torts* (9th ed, 1998) ch 19; 420.

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

164 *Ibid* 272–5. Creighton and Stewart discuss categorisations of work relationships and consider how various legislative frameworks such as OHS and anti-discrimination laws 'extend beyond the traditional concept of employment in a variety of ways'. It is the commission's view that this approach lends itself to the broadening of the concept of 'in the course of employment' to 'in the course of performing work'.

EXCLUSION OF THE WORKER'S HOME OR RESIDENCE

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

3.28 The effect of this exclusion is that practices affecting the privacy of workers in their homes will have to satisfy stricter requirements. An employer will be required to obtain an authorisation from the regulator before undertaking activities which affect workers' privacy in their homes. This requirement reflects the higher expectation of privacy which applies when workers are in their 'personal space'. It also takes account of the fact that employer acts or practices in the worker's home have the potential to affect the privacy of visitors to the home or other members of the worker's family. Employers may be able to justify acts or practices affecting workers at home, but they should have to make a case to the regulator before they can do so.

WORKERS USING AN EMPLOYER'S COMMUNICATION SYSTEM

3.29 The definition of work-related activities will include the situation when a worker is using the employer's communication system, regardless of where the worker is physically located.¹⁶⁵ This means that an employer will not be required to obtain an authorisation before monitoring the worker's use of the system.

3.30 The rationale for this approach is that employers' interests are affected by use of an employer-provided communications system, regardless of the workers' location or whether the system is being used to perform work-related or non-work-related activities. For example, an employer may be liable if a worker logs into the employer's email system from home and uses it to send sexually harassing emails to a co-worker. Employers also have a legitimate interest in preventing their communications systems from being used to download infringing copyright material from the internet. For this reason, the commission believes the employer is entitled to treat the use of a communication system as a work-related activity and to monitor use of that system, subject to any applicable advisory codes. This represents an exception to the exclusion of the worker's home or residence from the definition of work-related activities described in paragraphs 3.27–3.28.

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

BALANCING EMPLOYERS' AND WORKERS' INTERESTS AT WORK

3.31 The aim of the proposed workplace privacy legislation is to provide a minimum standard of privacy protection for workers without unduly limiting the ability of employers to run their businesses efficiently and competitively.¹⁶⁶ The commission recommends this aim be achieved by:

- imposing an obligation on employers not to use acts or practices which unreasonably breach workers' privacy when they are engaged in work-related activities;
- giving guidance on the scope of employers' obligations by including a statement of general principles in the legislation;
- providing for the regulator to issue advisory, and in some cases mandatory, codes of practice and to approve codes of practice prepared by employers.

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

EMPLOYERS' OBLIGATION

3.32 We recommend that the legislation prohibit employers from engaging in acts or practices that might unreasonably breach workers' or prospective workers' privacy. This obligation applies when the worker is engaged in work-related activities. The concept of 'unreasonableness' reflects the lower expectation of privacy in the work-related context. The inclusion of this provision qualifies the employers' obligation by allowing circumstances to be taken into account where employers have a legitimate need to use such acts or practices in the interests of their business. The use of such a concept was supported in a number of submissions,¹⁶⁷ including the Victorian Bar's:

If a right of privacy is found, the balancing of that right against competing rights or interests should also be based in reasonableness—the relative importance of the two sets of rights, whether there is any way of accommodating the competing rights without the privacy invasion, and if not, which should prevail.¹⁶⁸

166 Department of Treasury and Finance (2005), above n 144, 3-3.

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

168 Issues Paper submission 25.

PROVIDING GUIDANCE ON THE SCOPE OF THE OBLIGATION

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

3.34 One way would be to include detailed provisions in the proposed legislation dealing with all the practices which have the potential to affect workers' privacy. This is similar to the approach taken in the NSW Workplace Surveillance Act, which specifies the conditions under which surveillance can be conducted in the workplace.¹⁶⁹ We considered whether it would be desirable for the legislation to include detailed requirements for surveillance and internet and email monitoring. The commission rejected this approach because it would be inconsistent with our preference for using light-touch regulation rather than specific rules, except when dealing with certain practices which have a very serious effect on privacy. We were also concerned that provisions dealing with specific practices could rapidly become dated or defunct as a result of technological advances.¹⁷⁰

3.35 Another way would be to include broad principles governing particular practices in the legislation. These might be similar to the principles included in existing privacy legislation with which employers are already familiar.¹⁷¹ This approach was supported by some consultation participants.¹⁷²

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

169 *Workplace Surveillance Act 2005* (NSW) pt 2.

170 See Rachel Lebihan, 'Privacy law falling behind, inquiry told', *Australian Financial Review*, 7 March 2005, 13.

171 Roundtable 1.

172 *Ibid.*

the New South Wales Law Reform Commission (NSWLRC) in its Interim Report on Surveillance.¹⁷³

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

STATEMENT OF PRINCIPLES

3.38 A number of submissions commented on possible general principles.¹⁷⁴ One roundtable participant said that principles should be technology neutral and non-practice specific to ensure their ongoing relevance and effectiveness.¹⁷⁵ Some people suggested that general words and expressions in principles such as 'acceptable' and 'reasonable expectations of privacy' be avoided, or at least defined, to give employers guidance about how to comply with the principles.¹⁷⁶

3.39 Common themes in discussions were that employers should:

- have a legitimate purpose for which a practice is to be used;
- be required to determine whether less intrusive alternatives are available to the proposed practice;
- ensure the practices used are proportionate to the risk of harm they are seeking to avoid;
- review their use of practices regularly to determine whether they are still appropriate and necessary;
- consult with workers.¹⁷⁷

3.40 These themes were reflected in law firm Allens Arthur Robinson's submission:

173 NSWLRC (2001), above n 1, 179–93. The principles which the NSW commission recommended should apply to overt surveillance were not included in the *Workplace Surveillance Act 2005* (NSW).

174 See, eg, Options Paper submissions 4, 12, 22, 32.

175 Roundtable 4.

176 Options Paper submissions 4, 22.

177 See, eg, Options Paper submissions 4, 22, 24; roundtable 1. In Options Paper submission 32, an employer proposed that principles should also recognise that organisations can be vicariously liable and can owe a duty of care to their workforce, clients, customers or third parties and that accordingly an employer is entitled to be aware of its workers' activities.

We believe that the principles should encompass the concepts of reasonable expectation, acceptable purpose, proportionality and transparency. These concepts have formed the touchstone of workplace privacy legislation enacted in other jurisdictions both within Australia and overseas.¹⁷⁸

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

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

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

- for a purpose not directly connected to the employer’s business;
- in a manner that is not proportionate to the purpose for which the practice is undertaken;
- without first taking reasonable steps to inform and consult with workers;
- without providing adequate safeguards to ensure the act or practice is conducted appropriately having regard to the obligation not to unreasonably breach workers’ privacy.

3.44 These principles are broadly framed to allow employers the necessary degree of flexibility to deal with the diverse situations covered in this report¹⁷⁹ and the different problems which arise in the context of different types of work. We consider each principle below.

Purpose

3.45 Purpose is a fundamental aspect of information privacy regimes. The purpose for which information about an individual is collected generally determines what an

178 Options Paper submission 24.

179 See Chapter 1 paras 1.31–1.32.

organisation can subsequently do with that information.¹⁸⁰ Similarly, a consideration of the purpose for which a practice such as surveillance or email monitoring is used is an important first step in determining whether that practice is justified.¹⁸¹

3.46 In our first round of consultations, employers told us why they used video and other forms of surveillance, monitored workers' email and internet use, tested them for substances such as drugs and alcohol and used psychological tests in selection or promotion processes.¹⁸² Their reasons included:

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

3.47 As the practices engaged in to meet these purposes have the potential to invade a worker's privacy, we recommend the employer should have to show a direct connection between the practice and the operation of the employer's business. Establishing this connection assists in identifying the legitimacy of the purpose. The commission appreciates that employers are best placed to assess the nature of their particular business and the principle leaves it open to the employer to establish this connection. At the same time, the direct connection requirement offers a degree of protection to workers in ensuring the connection is not trivial or incidental in nature.

3.48 Examples of practices having a direct connection to the employer's business might include: the installation and overt use of surveillance cameras to prevent stock theft; use of an iris scanning device to control entry to the employer's premises; installing a software system to filter out emails containing trade secrets; or filtering workers' access to internet sites to prevent downloading of large files which will slow the operation of the employer's system.¹⁸³ By contrast, regular monitoring of employee

180 Generally, an organisation may use or disclose personal information for the primary purpose for which the information was collected, or for a related secondary purpose which the individual would reasonably expect. See, eg. *Privacy Act 1988* (Cth), sch 3, National Privacy Principle 2.1; *Information Privacy Act 2000* (Vic) sch 1, Information Privacy Principle 2.1(a); and in relation to health information, *Health Records Act 2001* (Vic) sch 1, Health Privacy Principles 2.1(a), 2.2(a).

181 Along similar lines, the NSWLRC proposed in relation to overt surveillance that it should only be undertaken for an acceptable purpose, see NSWLRC (2001), above n 1, 182.

182 VLRC (September 2004), above n 16, ch 3.

183 Options Paper submission 19. In its submission, Clearswift (internet and email software provider) states that in its research '50% of bandwidth is attributed to non-business-related information coming into or circulating throughout an organisation'.

emails to ensure workers are not expressing views contrary to the employer's religious beliefs or downloading images of workers from a video surveillance camera, simply because the workers are considered attractive, would not comply with this principle.

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

Proportionality

3.50 In the context of privacy, the principle of proportionality has been described as providing that 'any intrusion into an employee's privacy at work should be in proportion to the benefits of monitoring to a reasonable employer, which in turn, should be related to the risks that the monitoring is intended to reduce'.¹⁸⁴ Accordingly, this principle requires a balancing of the purpose and effect of the privacy infringement. If that purpose can be achieved in a way which is less intrusive than another act or practice, the employer would normally be expected to use the least privacy-intrusive measure.

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

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

It is important to ensure that whatever system is introduced in relation to workplace privacy, it does not further dilute employers' right to run their businesses as they consider appropriate. Clearly, protecting employee's privacy is also important, however, the reasonableness test based on proportionality would provide adequate protection.¹⁸⁵

3.53 The principle of proportionality also assists in engendering trust and confidence in the workplace when measures undertaken by employers are seen by staff

184 VLRC (October 2002), above n 3, para 5.7, for a further discussion of proportionality.

185 Options Paper submission 22.

as a balanced or measured response to a problem rather than 'overkill'. This was summed up in the Australian Human Resources Institute's submission:

The employer would need to think seriously about the benefits of secret surveillance because while, as a police tactic, it might provide a better chance of catching an offender, it can do great damage to workplace trust. Trust is a recurring critical factor in these cases because it is a lack of trust that gives credence to both employer suspicion and employee paranoia.¹⁸⁶

Taking Reasonable Steps to Inform and Consult Workers

3.54 The principle that workers should be informed and consulted about privacy-intrusive acts or practices reflects the fact that privacy is concerned with the protection of autonomy and dignity. Putting practices in place without informing workers about them and the reason the employer wishes to use them denies worker autonomy and is inconsistent with the implied duty not to engage in conduct that would undermine workers' trust and confidence.¹⁸⁷ Lack of knowledge that a particular practice is occurring also deprives workers of the opportunity to modify their behaviour. For example, workers who are regularly advised that their emails are being monitored may choose not to send personal emails which reveal private matters.

3.55 Apart from these principled reasons for informing and consulting workers, there are practical advantages in doing so. Provision of information and consultation with workers will help to educate them about the need to respect the privacy of co-workers and further encourage a healthy, respectful environment. Poor communication between employers and employees about practices which affect privacy may create industrial disputes. A sound consultation process assists in according procedural fairness to workers and is an important part of performance management systems generally. Communication with workers is required in other areas of law, including occupational health and safety law¹⁸⁸ and the federal industrial relations regime.¹⁸⁹

186 Issues Paper submission 16.

187 See VLRC (September 2004), above n 16, para 3.57, for discussion of this duty.

188 See roundtable 5; Options Paper submission 9. See *Occupational Health and Safety Act 2000* (NSW) pt 2, div 2; *Occupational Health and Safety Regulations 2001* (NSW), ch 3; *Occupational Health and Safety Act 2004* (Vic) pt 4. See also Chris Maxwell, *Occupational Health and Safety Act Review* (2004) 192.

189 Options Paper submission 4. For example, the *Workplace Relations Act 1996* (Cth) requires consultation on an agreement between an employer and a valid majority of the employer's employees before an agreement is certified: s 170LK(2). The Act requires employers to take reasonable steps to ensure that employees to

3.56 Informing or notifying individuals is also consistent with the approach taken under existing information privacy regimes,¹⁹⁰ which generally require organisations to take reasonable steps to notify people about their personal information-handling practices when or before information is collected (in the context of email monitoring, see, eg, the Australian Privacy Commissioner's *Guidelines on Workplace E-mail, Web Browsing and Privacy*).¹⁹¹

3.57 Many employers recognise the importance of transparent processes. A large employer told the commission that it includes information about surveillance, monitoring and testing practices in organisational policies and procedures, induction procedures and in regular communication updates.¹⁹² The organisation commented that, 'We are committed to a transparent approach with our employees in relation to all the practices we undertake, where possible'.¹⁹³

3.58 Some people also stressed the importance of incorporating an effective consultation mechanism into the regulatory regime.¹⁹⁴ As well as increasing the transparency of workplace practices, consultation may assist employers to identify ways of solving workplace problems that are less privacy invasive than the measures which the employer initially proposes. Consultation does not mean workers will have a right

whom the certified agreement will apply have 14 days written notice of the intention to make the agreement, and that the agreement must not be made until the 14 days have passed. The employer must take reasonable steps to ensure that those employees have access to the proposed written agreement at least 14 days before approval and to explain the terms of the agreement: s 170LK(3). The notice provided to the employees must state that if the employee is a member of an organisation entitled to represent the employee's industrial interests, the employee may request that the organisation represent the employee in meeting and conferring with the employer about the agreement: s 170LK(4). The employer must then give that organisation a reasonable opportunity to meet and confer with the employer about the agreement before it is made: s 170LK(5).

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

191 Office of the Privacy Commissioner [Aus], *Guidelines on Workplace E-mail, Web Browsing and Privacy* (30 March 2000) <www.privacy.gov.au/Internet/email/index.html> at 21 July 2005. The guidelines state: staff and management should know and understand the policy; guidelines should specify what is appropriate use and be explicit about what is and is not permitted; explain what information is logged and who has rights of access within the employer's operations; set out circumstances for disclosure of information; explain how the organisation intends to monitor and audit staff compliance with its policy; and review the policy on a regular basis to ensure it keeps up with technological development and re-issue the policy whenever changes are made.

192 Options Paper submission 27.

193 Ibid.

194 See roundtables 2, 3, 4, 5; Options Paper submissions 4, 9, 15, 23, 28, 32.

to veto practices which affect their privacy, but may assist in the formulation of procedures that accommodate more readily the concerns of both employers and workers.

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

3.60 Some employers were concerned that the requirement of consultation might prevent them from using covert surveillance to protect property from theft or to detect a worker engaged in illegal activities. One employer said that informing employees of all surveillance activities could jeopardise a legitimate investigation.¹⁹⁵ Paragraphs 3.82–3.90 recommend that the regulator should prepare codes regulating use of various types of covert surveillance by employers and that these codes should be binding on employers. The purpose of covert surveillance would be undermined if an employer had to inform particular employees that their activities were being secretly filmed or listened to. In this context, the principle that workers should be informed and consulted would be satisfied by informing workers in advance about the situations in which the employer might use covert surveillance and of the safeguards which would apply to its use.

Adequate Safeguards

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

- selection, training and qualifications of the personnel undertaking the practice;

195 Options Paper submission 27.

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

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

! RECOMMENDATION(S)

1. The legislation should provide that an employer must not engage in acts or practices that unreasonably breach the privacy of prospective workers or workers engaged in work-related activities.
2. An employer unreasonably breaches the privacy of prospective workers or workers if it engages in acts or practices:
 - for a purpose that is not directly connected to the employer's business;
 - in a manner that is not proportionate to the purpose for which those acts and practices are being used;
 - without first taking reasonable steps to inform and consult workers about the relevant act or practice;
 - without providing adequate safeguards to ensure the act or practice is conducted appropriately, having regard to the obligation not to unreasonably breach the privacy of the worker.
3. An act or practice is 'proportionate' under Recommendation 2 if it is the least privacy-invasive measure by which the intended purpose can be achieved.
4. The obligation to take reasonable steps to inform workers under Recommendation 2 requires provision of information to workers about:

! RECOMMENDATION(S)

- the nature of the act or practice and the reasons for introducing it;
 - the number and categories of worker likely to be affected;
 - the time when, or the period over which, the employer intends to engage in the act or practice;
 - the alternatives considered and the reasons why the alternatives were not considered appropriate;
 - the safeguards used to ensure the acts or practices are conducted appropriately.
5. The employer must take reasonable steps to give workers a genuine opportunity to influence the decision to introduce the act or practice.

CODES OF PRACTICE

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

3.64 There was considerable discussion in submissions and at roundtables about how codes could regulate workplace privacy. There were also differences of opinion about whether failure to comply with a relevant code should be regarded as a contravention of employers' obligation not to unreasonably breach the privacy of workers (in which case compliance with the code would be mandatory), or whether codes should only be used to give employers non-binding guidance on how to meet their privacy obligation. There were mixed views on this issue among employers.

3.65 Some employers and employer organisations¹⁹⁶ favoured advisory codes because they thought they would not impose excessive compliance costs and would provide guidance to employers without fettering their right to manage their workers.¹⁹⁷ It was

196 See Options Paper submissions 8, 15, 20, 24.

197 Roundtables 3, 4.

also argued that use of advisory codes was consistent with the approach taken to regulation in areas such as information privacy and workplace bullying.¹⁹⁸

3.66 Unions were more likely to support mandatory codes of practice¹⁹⁹ because of concerns that a 'softer' form of regulation would provide insufficient privacy protection to workers and place too much emphasis on employer perspectives and interests.²⁰⁰

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

ADVISORY CODES

3.68 We have recommended that employers should be under an obligation not to engage in acts or practices that unreasonably breach a worker's privacy, and that the content of this obligation should be determined by reference to four broad principles. We believe the regulator could provide guidance to employers by issuing advisory codes which clarify how various acts or practices can be undertaken in a way which complies with this obligation. Advisory codes could be drafted in a way which takes account of the needs and characteristics of different practices, different industries and different workplaces (eg the differences between small and big business). This approach allows the minimum regulation necessary to fulfil the social objective of privacy protection, while maximising business competitiveness and reducing possible administrative burden.²⁰¹ Of course, the obligation and principles would continue to apply to employers regardless of whether a code is issued.

3.69 Under our recommendations, advisory codes could be issued covering practices such as email and internet monitoring, psychological and medical testing of workers, use of biometric measures to control entry into buildings and the searching of workers and their belongings. Our recommendations will allow overt surveillance to be dealt

198 Options Paper submissions 12, 22; roundtable 3. See also the guideline making power in the *Privacy Act 1988* (Cth) s 27(e). An example of guidelines are the Office of the Privacy Commissioner [Aus] (30 March 2000), above n 191. See also *Occupational Health and Safety Act 2004* (Vic) div 3. An example of OHS guidelines are WorkSafe Victoria and Job Watch, *Workplace Violence and Bullying: Your Rights, What to Do, and Where to Go for Help* (2005).

199 Roundtable 3. See also Options Paper submission 4.

200 Options Paper submission 28.

201 Department of Treasury and Finance (2005), above n 144, 3-3.

with under an advisory code, but covert surveillance will be subject to stricter controls, which are discussed below.²⁰²

3.70 Issuing advisory codes is similar to the approach taken under many information privacy regimes. For example, the federal Privacy Commissioner has issued guidelines to help organisations comply with the National Privacy Principles contained in the Privacy Act. The guidelines include factors which the Privacy Commissioner may take into account when handling a complaint, but are advisory only and not legally binding.²⁰³ A similar approach is taken in the United Kingdom.²⁰⁴

3.71 Where the regulator has issued an advisory code and the employer has complied with it, we recommend this be conclusive evidence of compliance with the legislation and a sufficient answer to any complaint made about a breach of privacy. This is similar to the approach taken under the Victorian Occupational Health and Safety Act.²⁰⁵ Employers who have failed to comply with an advisory code issued by the regulator will be regarded as being in breach of the legislation, unless they can show they have taken other steps to comply with their obligation not to unreasonably affect workers' privacy.

3.72 As well as the regulator having power to issue advisory codes, we recommend it should have power to approve codes of practice developed by employers (or employer representative organisations) provided that these codes comply with the principles set out in Recommendation 2. For example, there may be scope for the retail industry to develop a retail video surveillance code, or the transport industry to develop codes on GPS tracking. Where the code has been produced by an employer and approved by

202 See paras 3.82–3.90 below.

203 *Privacy Act 1988* (Cth) s 27(1)(e), (ea). Cf *Privacy Act 1988* (Cth) s 16A, which prohibits an organisation from doing an act or engaging in a practice which breaches an approved privacy code which binds the organisation. See Office of the Privacy Commissioner [Aus], *Guidelines to the National Privacy Principles* (September 2001) <www.privacy.gov.au/act/guidelines/index.html#3.2> and *Guidelines on Privacy in the Private Health Sector* (November 2001) <www.privacy.gov.au/publications/hg_01.html> at 5 May 2005.

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

205 See *Occupational Health and Safety Act 2004* (Vic) ss 149–152.

the regulator, failure to comply with the code will be a breach of the employer's obligation not to unreasonably breach workers' privacy.

APPLICATION OF ADVISORY CODES TO JOB APPLICANTS

3.73 Job applicants²⁰⁶ are frequently required to have medical examinations or submit to psychological tests. Employers argue that these tools can assist in eliminating bias by increasing objectivity in assessments of people who are applying for a job.²⁰⁷ Such tests are meant to ensure that decisions are based on the ability to meet the requirements of the job and not on other irrelevant, or potentially discriminatory, factors.

3.74 Where information sought is directly relevant to the position, job applicants cannot legitimately object to practices which enable the employer to assess whether they are capable of performing the job on offer. However, the commission's Options Paper referred to a number of problems with psychological testing, including the use of inappropriate tests and their administration by people lacking relevant qualifications.²⁰⁸ While psychological tests may sometimes be useful, there are no legal requirements that ensure they will provide reliable information or be administered in an appropriate way. Job applicants may be required to answer invasive questions about private matters such as their social habits, likes and dislikes which have little or no relevance to their capacity to do the job.²⁰⁹

3.75 The Victorian Trades Hall Council limits its support of pre-employment testing to testing which relates directly to the skills required to perform the job.²¹⁰ Other unions advocate a total ban on pre-employment psychological and predisposition testing.²¹¹

3.76 The commission believes there are legitimate uses for reliable tests which provide employers with information directly relevant to the performance of the job. But this must be balanced against job applicants' right to protection against practices that unreasonably invade their privacy. People applying for a job are likely to find it difficult to refuse testing, even though the test has little relevance to their suitability

206 The recommendations also apply to other prospective workers, eg, people seeking a voluntary position.

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

208 VLRC (September 2004), above n 16, paras 2.38–2.92.

209 Consultation 4.

210 Options Paper submission 28.

211 See Options Paper submission 31; roundtable 2.

for employment. For this reason, we recommend that the regulator's power to issue advisory codes dealing with practices such as medical and psychological testing apply to job applicants and other prospective workers,²¹² as well as to people who are already working for the employer.

3.77 Later in this chapter, we make recommendations about drug and alcohol testing and the use of genetic information with respect to job applicants and other prospective workers.²¹³

- ! RECOMMENDATION(S)**
6. The regulator should have the power to issue advisory codes of practice to provide practical guidance to employers about how to fulfil the obligation imposed by Recommendation 1.
 7. Advisory codes may cover acts or practices which affect the privacy of workers or prospective workers while they are engaged in work-related activities other than:
 - acts or practices to which mandatory codes apply under Recommendation 14;
 - acts or practices which require authorisation under Recommendations 19, 22 and 25.
 - acts or practices which are prohibited under Recommendation 30.
 8. An advisory code of practice prepared by the regulator must be consistent with the principles in Recommendation 2.
 9. Compliance with an advisory code is conclusive evidence that the employer has complied with the obligation imposed by Recommendation 1.

212 Eg. people applying for internships or other voluntary positions.

213 See paras 3.91–3.96 (drug and alcohol testing) and paras 3.121–3.139 (genetic testing).

! RECOMMENDATION(S)

10. If an advisory code is in operation, contravention of the code is a contravention of the obligation imposed by Recommendation 1 unless the employer complies with that obligation in some other way.
11. The regulator should have the power to approve codes of practice (approved codes) prepared by employers that deal with acts or practices that affect the privacy of workers while they are engaged in work-related activities, other than:
 - acts or practices to which mandatory codes apply under Recommendation 14;
 - acts or practices which require authorisation under Recommendations 19, 22 and 25;
 - acts or practices which are prohibited under Recommendation 30.
12. The regulator may only approve a code which is consistent with the principles set out in Recommendation 2.
13. An employer must comply with an approved code of practice.

MANDATORY CODES

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

3.79 Which practices should be covered by mandatory codes? Our Occasional Paper *Defining Privacy* noted that the feelings of individuals vary widely as to whether particular activities amount to serious invasions of their privacy. The answer to this

question may differ according to the person's culture, the situation in which a practice occurs and the circumstances in which workers perform their jobs.²¹⁴ For example, a retail shop assistant, whose activities are observed by customers, may have different expectations of privacy from workers in an office on their own. But the existence of these differing expectations is not an argument for failing to protect privacy.²¹⁵ *Defining Privacy* argued that there is a public interest in protecting human beings from activities which undermine workers' autonomy and dignity, because such activities undermine their status as human beings.²¹⁶

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

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

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

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

Covert Surveillance

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

214 Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*, Report No 67 (1995) 42.

215 Ibid.

216 Foord (2002), above n 13, 40.

3.83 By covert surveillance we mean video surveillance, use of a listening device such as a tape recorder, tracking technology such as a GPS device²¹⁷ and monitoring of email or internet use that is undertaken without a worker being notified of the surveillance. For example, covert video surveillance occurs when an employer films a worker on a hidden camera without informing the worker of the surveillance. Covert email surveillance occurs when emails sent or received by workers are monitored without workers being aware it is occurring.

3.84 The issue of whether covert surveillance should be treated differently from overt surveillance attracted some comment in submissions and at roundtables. Some unions argued that both overt and covert surveillance can be objectionable, depending on the context.²¹⁸ Concerns were expressed about the increasing use of overt surveillance to monitor workers' productivity. We were told this was becoming pervasive in some areas of work, such as call centres.²¹⁹ Unions said overt surveillance was being used as a substitute for good staff management and it reduced trust in the workplace and contributed to worker stress and breakdown.²²⁰ On this basis, unions argued that both overt and covert surveillance had the potential to severely affect workers and that notifying a person that surveillance was being used did not reduce this effect.²²¹

3.85 The commission believes some concerns about excessive use of overt surveillance are justified and this use can severely affect workers' autonomy and dignity. The regulator will have power to publish advisory codes governing this kind of surveillance. In our view, however, the use of surveillance generally to monitor and increase workers' productivity raises issues about working conditions which are not limited to the protection of workers' privacy. It may be preferable to deal with conflicts about intrusive productivity monitoring within a broader industrial relations

217 These terms are defined in the *Surveillance Devices Act 1999* (Vic) s 3.

218 Roundtable 2.

219 See, eg, roundtable 5, consultations 15, 6, 21.

220 See, eg, Issues Paper submission 2, in which the Australian Honesty Forum states, 'surveillance can impinge on mental, rather than physical, health. When employees are monitored, they feel the need to suppress their emotions and opinions continuously. They fear the expression of their genuine feelings could jeopardise their position or status. This continuous suppression of emotions and opinions tends to induce burnout—a sense of mental exhaustion and alienation'. In Issues Paper submission 5, a former call centre worker said 'I found this to be an extremely stressful environment and eventually the pressure got to me and I could no longer continue. Many other people I spoke to found it stressful to be monitored so heavily'.

221 Options Paper submission 5.

framework, rather than simply as a privacy matter.²²² In Chapter 4 we propose that the regulator have the power to decline a privacy complaint if it would be more effectively dealt with in another forum.

3.86 Other stakeholders thought that covert surveillance should be subject to some kind of authorisation mechanism because it was more intrusive than overt surveillance.²²³ It was suggested that employers should not have greater powers to undertake covert surveillance than the police, who are generally required to obtain a warrant to undertake such activities.²²⁴ It was also suggested that if employers suspect unlawful activity they should be required to seek police assistance rather than trying to catch the perpetrators themselves. Employers thought this would create difficulties as the police may not have the time and resources to investigate all suspected activities. Employers were also concerned that having to seek some kind of authorisation before using covert surveillance could lead to loss of evidence due to potential delays in obtaining an authorisation.²²⁵

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

222 An example of this is the use of 'mystery shoppers'. This practice was raised as a privacy issue on a number of occasions during our consultations, but has more to do with the use of a particular kind of performance-management practice than an issue of workplace privacy: consultation 6

223 Roundtable 3; Options Paper submissions 4, 14, 30, 32.

224 Roundtable 5. See, eg, *Surveillance Devices Act 1999* (Vic) pt 4, which sets out the requirements in relation to warrants for the use of surveillance devices by law enforcement officers.

225 Roundtable 5.

the privacy of a person to whom the worker sends the email as well as of the worker. Likewise, covert use of video surveillance affects people who visit the workplace.

3.88 The NSWLRC has pointed out that covert surveillance may discriminate against groups such as low paid workers, who are more likely to be its targets, and it may also result in the targeting of 'certain individuals or groups', such as union members.²²⁶ In NSW, the need to control covert surveillance has been recognised by legislative provisions which require authorisation to be obtained from a magistrate before surveillance is undertaken.²²⁷

3.89 The commission considered the NSW approach of requiring an employer to obtain authorisation from a magistrate before using covert surveillance.²²⁸ However, we believe requiring employers to comply with mandatory codes on surveillance is a more appropriate way of achieving the necessary balance between the interests of employers and the privacy of workers. The NSW requirement of obtaining an authorisation from a magistrate deals with covert surveillance on a case-by-case rather than systemic basis. In our view, mandatory codes are more likely to produce a systemic change in employer practices. They can deal with issues such as:

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

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

226 NSWLRC (2001), above n 1, 287.

227 *Workplace Surveillance Act 2005* (NSW) pt 4, divs 1, 2.

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

Drug and Alcohol Testing

3.91 Drug and alcohol testing is now used in a number of industries in Australia, although there are no recent statistics on the extent of its use.²²⁹ Some organisations which made submissions or attended roundtables said such testing should be prohibited or only allowed in specified situations.²³⁰ The commission does not support an outright prohibition of these practices as it believes their use may be justified in some situations for occupational health and safety reasons. This is particularly so given the inclusion of drug and alcohol testing programs in some federal industrial agreements (which have the force of federal law).²³¹ In the commission's view, drug and alcohol testing should be subject to mandatory codes. Stricter control of these practices is necessary because of their invasiveness, the potential for misuse of information obtained from them and the varying reliability of these tests.

3.92 The process of drug and alcohol testing is inherently intrusive because it involves the taking of bodily samples. The most common forms of testing involve breath testing for alcohol and urine testing for drugs. The taking of saliva samples is also becoming common. Blood testing may be required to confirm the results of other less accurate tests. Privacy is often characterised as relating to an individual's autonomy and dignity and the concept of bodily privacy is integral to this.²³² Taking bodily samples erodes the distinction between the privacy of workers' bodies and the obligations they owe to their employers. There is nothing except the cost of testing to stop employers requiring workers to submit to weekly tests of their urine, blood or saliva as a condition of employment. The results of these tests may have little or no relevance to workers' capacities to do their job. Many unions objected to random drug and alcohol testing. The Shop, Distributive and Allied Employees' Association said in its submission that 'testing must be incident based, not random and should only relate to impairment'.²³³

3.93 Another reason for applying mandatory codes to drug and alcohol testing is that these tests can provide a great deal of private information. Drug testing in particular has the potential to reveal information about a worker's, or prospective

229 Australian Law Reform Commission, *Essentially Yours: the Protection of Human Genetic Information in Australia, Volume 2*, Report No 96 (2003) 762.

230 In roundtable 5 it was suggested that drug and alcohol testing should be prohibited with exemptions for particular cases such as drug testing of airline pilots.

231 See VLRC (September 2004), above n 16, para 2.90.

232 See Australian Law Reform Commission, *Privacy*, Report No 22 (1983) vol 1, 21.

233 Options Paper submission 9.

worker's, private life. Such tests might, for example, reveal that a worker is taking prescription drugs to treat a particular disease, which the worker wishes to keep private and which may be irrelevant to his/her capacity to do the job.

3.94 Tests may also reveal that workers have taken a recreational drug in their own time.²³⁴ Unions have expressed concern that employers might act as 'de facto police'²³⁵ in monitoring workers' drug and alcohol consumption after hours, when it may have little or no effect on their work performance.

3.95 Finally, the reliability of these tests also varies. The process of drug and alcohol testing is largely unregulated and there is no requirement on the employer to put steps in place to ensure the accuracy of the test or to require bodily samples to be analysed by an accredited laboratory.²³⁶

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

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

3.97 The commission has included consent as a requirement in the mandatory code because consent must be sought when a bodily sample is removed—otherwise it would

234 See VLRC (September, 2004), above n 16, paras 2.72–92 for a discussion about the processes of drug and alcohol testing.

235 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, Sydney, 5 December 2002) 3.

236 See VLRC (September, 2004), above n 16, paras 2.74, 2.77, 2.92, which discuss accreditation of laboratories in relation to drug and alcohol testing. For further discussion of issues in drug and alcohol testing, see *ibid* paras 2.72–2.92, 3.52–3.101.

constitute assault (this requirement would similarly apply to medical and genetic testing).

Other Prescribed Practices

3.98 Technology is evolving at a rapid rate and community attitudes to particular practices change over time. For these reasons, the commission believes the proposed legislation should contain a provision enabling other practices to be regulated by mandatory codes. We recommend that the legislation allow regulations to be made requiring other practices to be covered by mandatory codes prepared by the regulator. Such new practices may come to light through the complaints system or through the regulator's investigation powers, which are discussed in Chapter 4. In that chapter we recommend that one of the regulator's functions should be to monitor technological developments to assess the impact on workers' privacy. This is also consistent with the *Victorian Guide to Regulation* requirement that regulation should be constantly evaluated to ensure the specified social and equity objectives are being met.²³⁷

3.99 Another rationale for enabling other practices to be regulated by mandatory codes is that it provides an escalating mechanism if employers do not follow their advisory code obligations. If employers fail to meet their obligations under the light-touch regulatory regime, the regulator may recommend the practice in question be prescribed and made subject to more onerous mandatory regulation.

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

3.101 One practice which may be worth monitoring²³⁸ is the potential use of radio frequency identification (RFID) chips to track or monitor individuals.²³⁹ It was recently reported that the US Food and Drug Administration had approved the use of

237 Department of Treasury and Finance (2005), above n 144, 3-3.

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

239 RFID 'is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached or incorporated into a product. RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transponder': <<http://en.wikipedia.org>> at 5 May 2005.

RFID chips in hospital patients to improve patient care.²⁴⁰ The chips can be injected into the fatty tissue of patients' arms and a scanner can be used to obtain information about their blood type, identity and condition.

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

Job Applicants and Other Prospective Workers

3.103 The commission recommends that mandatory codes for drug and alcohol testing cover the testing of job applicants and others who are seeking positions as independent contractors or volunteers (prospective workers), as well as people who are already workers. This is because a job applicant or other prospective worker may be placed in the position of consenting to a privacy-invasive act or practice or missing out on the job altogether. This issue was identified in the report of the Privacy Committee of New South Wales into workplace drug testing, which acknowledged that consent is virtually meaningless in the pre-employment context.²⁴¹ Evidence of the difficulty which job applicants face in refusing a test was reflected in an employer representative's comment to the commission that there was generally no resistance to pre-employment testing.²⁴²

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

240 Munir Kotadia, *Subcutaneous RFID tags upset privacy advocates* (15 October 2004), ZDNet UK <<http://news.zdnet.co.uk>> at 15 October 2004.

241 See Privacy Committee of New South Wales, *Drug Testing in the Workplace*, Report No 64 (1992) 12.

242 Consultation 10.

! RECOMMENDATION(S)

14. The regulator must issue mandatory codes of practice about the following acts or practices:
 - covert surveillance of workers in the workplace (including covert use of optical surveillance devices and of listening or tracking devices and covert surveillance or monitoring of emails or internet use);
 - the taking of bodily samples from workers or prospective workers for the purposes of drug and alcohol testing;
 - any other acts or practices that are prescribed by regulation for the purposes of this section.
15. A mandatory code of practice must be consistent with the principles in Recommendation 2.
16. In deciding whether to issue a mandatory code the regulator should consult with relevant organisations and persons.
17. A mandatory code of practice, or a variation or revocation of a mandatory code of practice, must be approved by the relevant minister.
18. An employer who fails to comply with a mandatory code breaches the obligation imposed by Recommendation 1.

PRIVACY PROTECTION FOR WORKERS WHEN NOT WORKING

3.105 Recommendations 1 to 18 are intended to balance the interests of employers and the privacy interests of workers when they are involved in work-related activities. However, we argued in paragraphs 3.14–3.22 that workers should receive greater privacy protection when they are not working.

3.106 Because workers are not ‘owned’ by their employers, they have the same privacy interests when they are not working as everyone else. The fact that a person is an employee, an independent contractor or a volunteer should not qualify a reasonable expectation of privacy outside the work context. As the Privacy Committee of NSW

has commented, 'it is important for people to be able to preserve a distinction between their public and private worlds'.²⁴³

3.107 It follows that employers should not normally use acts or practices which affect workers' privacy when they are not working. The commission's Occasional Paper *Defining Privacy* argued that privacy is not just a matter of individual concern but a condition of existence as a human being. Interference with workers' rights to enjoy a social life outside work erodes their humanity and treats them as if they are owned by their employers. For this reason, it will usually be inconsistent with the public interest to allow employers to attempt to monitor the activities or movements of a worker outside working hours.²⁴⁴ There is little evidence of the extent to which this is currently occurring, but during the course of the reference we were given some examples. For instance, we were told that private detectives were sometimes hired by reputation-sensitive employers to place executive workers under surveillance to discover whether they were having an affair, or to ascertain whether a worker was selling property stolen from the employer.

3.108 Although employers should not normally use acts or practices which affect the privacy of workers outside work, we do not think the complete prohibition of such practices is justified. Some incursion into workers' lives may be warranted when a worker does something outside work that has a direct effect on work responsibilities. For example, the fact that a member of the police force is associating with criminals out-of-hours or that a teacher is having a sexual relationship with an under-age student is directly relevant to their work.²⁴⁵ Where such behaviour is suspected, it may be legitimate for an employer to put measures in place to determine whether these acts are occurring.

3.109 There are also situations where it is practically impossible to use technologies which affect the worker's privacy in the context of work, without also having some effect on the worker's private life. For example, an employee may be provided with a

243 Privacy Committee of New South Wales (1995), above n 214, 41.

244 Foord (2002), above n 13, 40.

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

car to be used both for work and private purposes. The car may have a GPS device installed in it, which enables the employer to track the worker's movements out-of-hours as well as during working hours. There may be difficulties in ensuring the device is deactivated at times when the worker is not working. In this situation it may be preferable to place conditions on access to and use of information about the worker's out-of-hours movements, rather than preventing use of GPS devices altogether.

3.110 Our approach begins with the assumption that it is an important social objective that employers not invade a worker's privacy when the worker is not working. Where the employer argues there is a justification for doing so, the employer should be required to displace this assumption and show that the act or practice is proportionate to the protection of the employer's interest, having regard to the higher expectation of privacy which workers have in relation to their private lives.²⁴⁶

AUTHORISATION REQUIREMENT

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

3.112 The authorisation process will require the employer to 'build a case', and demonstrate to the regulator the need for such an act or practice. For example, why an employer wishes to log GPS tracking of company-provided cars outside of work hours, or why the employer needs to place an employee suspected of theft under after-hours surveillance.²⁴⁷ The regulator may authorise the act or practice if satisfied that:

246 An argument against using a distinction between public and private as the conceptual basis for the model is the underlying assumption that greater privacy protection attaches to the 'private domain' even though certain 'public acts' may warrant a high degree of privacy protection (for a general discussion of these concepts see Foord (2002), above n 13, 38–41; Victorian Law Reform Commission, *Privacy Law: Options for Reform* (2001) paras 3.1–3.25). The proposed workplace privacy legislation moves beyond the parameters imposed by the distinction between public and private by relying instead on whether or not work is being performed. This approach reflects the complex nature of the modern work relationship which traverses both public and private domains. The performance of work can, for example, occur in the so-called private domain of the home. Conversely, highly privacy-invasive activities can occur in the public domain of the workplace. Accordingly, the prescribed level of regulation is not determined solely by whether the act occurred in the public or private domain, but rather focuses on whether or not work is being performed (assessed against other considerations such as the degree of the privacy invasiveness of the practice).

247 Roundtables 1, 2.

- the worker's out-of-hours activity has the potential to have a direct and serious impact on the business or reputation of the employer;
- the act or practice affecting privacy cannot reasonably be undertaken while the worker is engaged in work-related activities;
- the effect of the act or practice on the worker's privacy is proportionate to the protection of the employer's interests, having regard to the higher expectation of privacy which applies to workers when they are not working;
- the employer will inform and consult workers concerning the act or practice and will ensure the act or practice is conducted appropriately;
- adequate safeguards have been put in place to minimise the breach of a worker's privacy.

3.113 These criteria give employers guidance on what they must demonstrate to the regulator in seeking an authorisation, and make transparent the factors which the regulator will take into account in authorising the act or practice. The criteria will also contribute to the development of minimum standards to protect workers' higher expectation of privacy in the non-work-related context. Where an employer engages in an act or practice in the non-work-related context without an authorisation, a civil penalty applies (see paras 4.81–4.88 for further detail). One of the regulator's functions is to issue guidelines to assist employers in preparing for an authorisation. We believe, given the seriousness of the social objective at stake, this form of regulation is justified to ensure the desired regulatory outcome.²⁴⁸

DRUG AND ALCOHOL TESTING

3.114 We have recommended that drug and alcohol testing of workers involved in work-related activities be regulated by mandatory codes. There are some situations where an employer may wish to monitor the drug intake of workers when they are not working. Some sporting organisations are required to randomly drug test athletes in order to meet international requirements for sporting events.²⁴⁹ Sporting and other

248 Department of Treasury and Finance (2005), above n 144, 3-3, 3-7.

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

organisations may also argue that they are entitled to ‘protect their image’ by monitoring athletes’ or workers’ drug or alcohol consumption outside the work context.²⁵⁰ Workers may be placed under pressure to consent to monitoring at times when they are not working.

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

! RECOMMENDATION(S)

19. The legislation should provide that an employer must not engage in acts or practices that breach the privacy of a worker when the worker is engaged in non-work-related activities without an authorisation from the regulator.
20. The regulator may authorise the employer to engage in an act or practice which affects the privacy of a worker engaged in non-work-related activities, if the regulator is satisfied that:
 - there are reasonable grounds for believing the worker’s out-of-hours activity may have a direct and serious impact on the business or reputation of the employer;
 - the employer’s act or practice affecting privacy cannot reasonably be undertaken while the worker is engaged in work-related activities;
 - the act or practice is a proportionate response to the protection of the employer’s interests;
 - the employer will inform and consult workers concerning the act or practice and ensure the act or practice is conducted appropriately;

the NRL and the AFL have sport-specific illicit drug codes. The NRL policy allows for testing for illicit drugs in the workplace during training and competition seasons. The AFL code allows for out-of-competition testing for illicit drugs.

! RECOMMENDATION(S)

- adequate safeguards have been put in place to minimise breaches of workers' privacy.

21. An employer may seek a review by VCAT of the regulator's decision to authorise or refuse to authorise.

OTHER PRACTICES REQUIRING AUTHORISATION

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

- acts or practices affecting privacy in workers' homes;
- genetic testing;
- other prescribed practices.

PRIVACY IN WORKERS' HOMES

3.117 A substantial percentage of workers do all or some of their work at home. The trend towards home-based work is increasing.²⁵¹ In Victoria, the Surveillance Devices Act prohibits a person from using, installing or maintaining optical surveillance and listening devices to record private conversations or private activities to which that person is not a party, except with the consent of the person affected.²⁵² Many activities and conversations occurring within a worker's home will come within the definition of private activities and conversations under the Surveillance Devices Act.²⁵³ Nevertheless, the employer can listen to or film workers in their homes if the workers consent. Some

251 Marilyn Pittard, 'The Dispersing and Transformed Workplace: Labour Law and the Effect of Electronic Work' (2003) 16 (1) *Australian Journal of Labour Law* 69, 74–5.

252 *Surveillance Devices Act 1999* (Vic) s 6.

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

workers may feel under pressure to agree to the employer using such devices in their homes.

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

3.119 In the commission's view, workers are entitled to greater privacy protection in their home than in other situations. As one submission stated, 'The employer has no business interfering with the privacy of the employee's home'.²⁵⁴ Even when engaged in work-related activities, acts or practices engaged in by an employer which relate to the worker's employment or engagement may also affect the worker's private life. In addition, use of practices such as surveillance in a worker's home are likely to affect the privacy of other people who live there, for example the partner and children of the worker.

3.120 This approach is consistent with the NSW approach contained in the Workplace Surveillance Act. One important difference is that the NSW Act imposes a complete prohibition on using a work surveillance device while the employee is not at work (with the exception of computer surveillance of employer-provided equipment and resources). Non-compliance is a criminal offence.²⁵⁵ In comparison, we believe our proposed model offers a more flexible regulatory outcome in allowing employers to apply for an authorisation from the regulator. Failure to seek or comply with an authorisation is subject to a civil penalty (see 4.81–4.88 for the commission's rationale on using civil penalties).

254 Issues Paper submission 9.

255 *Workplace Surveillance Act 2005* (NSW) s 16(1), which states, 'An employer must not carry out, or cause to be carried out, surveillance of an employee of the employer using a work surveillance device when the employee is not at work for the employer unless the surveillance is computer surveillance of the use by the employee of the equipment or resources provided by or at the expense of the employer'. Maximum penalty: 50 penalty units.

! RECOMMENDATION(S)

22. An employer must not use acts or practices which affect workers' privacy while they are working at home, unless the act or practice is authorised by the regulator.
23. The regulator may authorise an employer to use acts or practices which affect the privacy of workers while they are working at home if the regulator is satisfied of the matters set out in Recommendation 20.
24. An employer should not be required to seek an authorisation to monitor a worker's email or internet use when the worker is using the employer's communication system, wherever the worker is situated.

GENETIC TESTING

3.121 The commission did not discuss the issue of privacy and genetic testing in the Options Paper²⁵⁶ because this issue was then being considered in the joint Australian Law Reform Commission–Australian Health Ethics Committee's (ALRC–AHEC) inquiry into the protection of human genetic information. For this reason, we go into some detail here about the issues relating to genetic testing.

3.122 A number of participants in our consultations raised concerns about genetic testing in the workplace.²⁵⁷ In this section, we recommend that employers be required to obtain an authorisation from the regulator before undertaking genetic testing of a worker or prospective worker. In discussing this issue, we draw upon the ALRC–AHEC's comprehensive report.²⁵⁸

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

256 See VLRC (September 2004), above n 16, para 1.9.

257 See, eg, Options Paper submissions 9, 28, 31.

258 Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia: Volume 1*, Report No 96 (2003); Australian Law Reform Commission (2003), above n 229, vol 2.

deals with the processes by which genetic information²⁵⁹ is obtained (this includes both genetic testing and taking a person's family medical history), the purpose for which the information is used and the privacy protection which applies to it. In keeping with our practice-based approach, our primary concern relates to employers requiring workers to have genetic tests.²⁶⁰ This may be done by requiring a job applicant or worker to have a genetic test or to give the employer access to bodily samples for this purpose.

GENETIC TESTING IN EMPLOYMENT

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

- Genetic tests may be included in pre-employment health screening of workers to identify whether a person has a disease or other condition, or has a genetic predisposition to develop a disease or condition.²⁶¹
- Genetic tests of workers can be used as part of an ongoing health surveillance program. Health surveillance designed to detect whether a person has suffered genetic damage as the result of exposure to hazardous substances, such as lead, is required in some industries.²⁶²
- Genetic tests may be used for the purposes of identification in a few industries. For example, police forces may want officers to provide DNA samples to eliminate the possibility their DNA has contaminated a crime scene.²⁶³

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

259 Genetic information may be obtained in ways which do not involve genetic testing, eg by taking a family medical history from a person. In addition, workers may provide blood and other bodily samples as part of a health examination. Employers might seek access to these samples to obtain genetic information: ALRC (2003), above n 229, vol 2, 762–4, paras 29.16–21.

260 Ibid.

261 ALRC (2003), above n 229, vol 2, 760–761; paras 29.5–29.7.

262 Ibid 761, paras 29.8–10.

263 Ibid 765, paras 29.27–30. We are informed by Victoria Police that its current policy is that collection of DNA samples for the purpose of excluding members from a crime scene can only occur if the member consents to it.

It is difficult to predict to what extent Australian employers may seek to obtain and use genetic information about job applicants or employees in the future. Australian employers already undertake a wide range of employee health assessments on a routine basis and may in future make use of genetic information as part of their pre-employment health assessment, or as part of ongoing health surveillance under occupational health and safety regulation.²⁶⁴

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

Concerns about genetic screening are magnified once account is taken of future gene chip analysis and the potential for testing for a range of non-medical traits, such as aggression, alcoholism or criminality; traits that an employer would undoubtedly be keen to screen for.²⁶⁵

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

REGULATION OF GENETIC TESTING OF WORKERS

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

- no legal requirement to inform the individual about the purpose for which a sample may be used or to whom the sample may be transferred when consent is obtained to testing;²⁶⁶
- limited protection against collection and genetic testing of bodily samples obtained without consent (eg by DNA testing a strand of hair),²⁶⁷
- failure of the federal Privacy Act to cover genetic samples, even when they identify an individual;²⁶⁸

264 Ibid para 29.32.

265 Margaret Otlowski, *Implications of Genetic Testing for Australian Employment Law and Practice* (2001) 9.

266 Ibid 11–13.

267 ALRC (2003), above n 258, vol 1, 362–364, paras 12.16–26.

268 Ibid 261, para 8.2. For detailed discussion of the reasons that genetic samples are not protected see ch 8.

- the exclusion of personal information contained in ‘employee records’, including genetic information from privacy protection under the federal Privacy Act;
- failure of anti-discrimination laws to prohibit discrimination against job applicants or workers because they have a genetic predisposition to develop a disease or disability²⁶⁹ or on the basis of genetic characteristics which are not a disability but are considered undesirable by an employer (eg a tendency to be aggressive or shy).²⁷⁰

3.128 Victorian laws also deal inadequately with these issues. The Victorian Equal Opportunity Act prohibits discrimination in the area of employment based on the fact that a person has an existing disability or disease but may not cover the case where a person has a genetic predisposition to develop a disability or disease, or has other genetic tendencies considered undesirable by an employer.²⁷¹

3.129 The Health Records Act protects the privacy of ‘health information’, which is defined as including ‘other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or any of his or her descendants’.²⁷² However, this does not appear to cover genetic information which may be used in the future to identify traits which are not relevant to health, such as a tendency to be aggressive.²⁷³

ALRC–AHEC RECOMMENDATIONS

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

- amending discrimination laws to cover collection, use and requests for genetic information and to exclude genetic predisposition or future genetic status from the ability to perform work;²⁷⁴

269 Ibid 305–307, paras 9.71–79.

270 See Otlowski (2001), above n 265.

271 *Equal Opportunity Act 1992* (Vic) s 4 has a definition of ‘impairment’. Note that this covers the presence in the body of organisms that may cause a disease, but may not cover genes which may cause a disease.

272 *Health Records Act 2001* (Vic) s 3 for the definition of personal information.

273 Otlowski (2001), above n 265, 9.

274 ALRC (2003), above n 229, vol 2, 783, Recommendation 30-1; 792, Recommendation 31-1; 800, Recommendation 31-3. In Victoria, this would require amending the *Equal Opportunity Act 1995* to prohibit discrimination against people because they have a genetic predisposition to develop an impairment or to manifest other physiological or psychological attributes, except where this would be permitted under

- establishing a Human Genetics Commission to make recommendations about genetic tests for screening susceptibility to particular work-related conditions;
- developing national codes for conduct of genetic screening, genetic monitoring of employees exposed to hazardous substances and assessment of workers' compensation claims;²⁷⁵
- amending the employee records exception in the federal Privacy Act to ensure the Act protects the privacy of genetic information contained in employee records;²⁷⁶
- developing a criminal offence to cover non-consensual genetic testing.²⁷⁷

AUTHORISATION REQUIRED FOR GENETIC TESTING

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

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

3.133 Genetic testing has the potential to severely affect workers' privacy and autonomy. Requiring a worker to undertake a test may reveal information they may not wish to know, for example, the fact that they may develop a serious disease. Genetic testing can provide information not only about the individual worker, but also about the worker's blood relatives. The potential for genetic samples to be analysed to reveal more and more information will increase as genetic technology develops. This will enable employers to discriminate against workers who have a genetic predisposition to develop a disability or a disease, or who have other genetic characteristics. The ALRC–AHEC report found that while these uses of genetic

other provisions of the Act. This amendment would cover discrimination on genetic grounds, whether genetic information is obtained from a test or by simply taking a medical history.

275 ALRC (2003), above n 229, vol 2, 817, Recommendation 32-2; 822, Recommendation 32-4; 841, Recommendation 33-1.

276 Ibid 841, Recommendation 33-1.

277 Ibid 374, Recommendation 12-1.

information are not yet widespread, complaints about discrimination are beginning to emerge.²⁷⁸

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

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

- a worker with a genetic deficiency might be more susceptible to a particular hazard than other workers (eg workers with a genetic deficiency in the production of a particular protein are more susceptible to lung disease in dusty environments);²⁷⁹
- workers are exposed to a workplace hazard such as a toxic chemical or radiation and they need to be monitored to detect the genetic effects of this exposure;²⁸⁰
- genetic screening may assist in the protection of third parties;²⁸¹
- strong evidence exists of a connection between the working environment and the development of a particular condition;
- there is evidence that a condition may seriously endanger the health of an employee or the health and safety of third parties;
- there is a scientifically reliable method of screening for a condition.²⁸²

278 Ibid.

279 ALRC (2003), above n 229, vol 2, 808, paras 32.19–21.

280 Ibid 818, para 32.54.

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

282 The last three requirements reflect the approach recommended in the ALRC (2003), above n 258, vol 1, 67–9.

3.136 The employer should also have to show there are no other reasonable means to eliminate or reduce the hazard which genetic testing seeks to eliminate or reduce. This is consistent with the proposed principle that acts or practices which affect the privacy of workers should be proportionate to the purpose for which those acts and practices are being used.

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

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

3.139 In this context, the definition of worker includes job applicants and other prospective workers. We have argued that the capacity of job applicants to refuse to submit to acts and practices that breach their privacy is illusory.²⁸³ For this reason, we believe it is appropriate to require authorisation before employers can use bodily samples to obtain genetic information about the characteristics of job applicants.

! RECOMMENDATION(S)

25. An employer must not conduct genetic testing of workers or prospective workers unless genetic testing is authorised by the regulator.
26. The regulator may authorise an employer to undertake genetic testing of workers if the regulator is satisfied that:
 - workers have consented to being genetically tested;
 - there is substantial evidence of a connection between the working environment/workplace hazard and the existence or predisposition to a condition which may be detected using genetic testing;
 - the condition or predisposition which may be detected has the potential to seriously endanger the health and safety of the worker or a third party;

283 See paras 3.103–3.104.

**RECOMMENDATION(S)**

- there are no other reasonable means by which the hazard, which genetic testing seeks to eliminate or reduce, can be eliminated or reduced;
- there are no other reasonable means of detecting a condition;
- the proposed genetic test is scientifically reliable;
- the employer has put in place adequate safeguards to ensure tests are conducted appropriately;
- the employer has taken appropriate steps to ensure any information obtained as a result of the test will be adequately protected from disclosure;
- the employer has taken reasonable steps to inform and consult with workers about the conditions under which the genetic testing will be undertaken.

27. Genetic testing means the use of samples obtained from the body of a worker, or prospective worker, for the purposes of obtaining genetic information about the worker or prospective worker.

AUTHORISATION REQUIRED FOR OTHER PRESCRIBED PRACTICES

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

**RECOMMENDATION(S)**

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

FAST-TRACKING AUTHORISATIONS

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

! RECOMMENDATION(S)

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

PROHIBITED PRACTICES

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

It is important for people to be able to preserve a distinction between their public and private worlds. The private world includes the employee's beliefs, personal habits and conduct relating to their own body such as visiting the toilet and changing clothing.²⁸⁴

3.143 The commission believes surveillance of workers in toilets, change rooms, lactation rooms or wash rooms is an affront to community expectations and should be prohibited. Under the Surveillance Devices Act, it is a criminal offence to install, use or maintain a listening device to listen to or record a private conversation to which the person using the device is not a party, and to install, use or maintain a video surveillance device to record visually or observe a private activity to which the person using the device is not a party.²⁸⁵ It is also an offence to publish a record of a private conversation or private activity made as the result of the use of a listening device or

284 Ibid 41.

285 *Surveillance Devices Act 1999* (Vic) ss 6–7.

optical surveillance device, without the express or implied consent of each person involved in the private activity or conversation.²⁸⁶

3.144 As paragraph 1.27 explains, the Surveillance Devices Act provides limited protection to workers because conversations and activities in the workplace will often not come within the definition of ‘private conversations’ and ‘activities’. What a worker does in a toilet or change room is likely to be regarded as a ‘private activity’. However, the Surveillance Devices Act does not prohibit surveillance in such areas if the worker consents to it. In our view, it is inappropriate for workers to be asked by an employer to consent to surveillance in such areas.

3.145 A similar prohibition to that which the commission proposes is contained in the NSW workplace surveillance legislation.²⁸⁷ Some of the organisations and individuals we consulted also specifically referred to the unacceptability of this practice.²⁸⁸ The Victorian Trades Hall Council submission advocated:

The listing of physical locations in which breaches of privacy cannot be allowed for any reason because the nature of the breach would contravene most, if not all, of the fundamental requirements for privacy—autonomy, dignity, workers not to be treated as objects and have the capacity to form and maintain their social relationships in the workplace. Whilst not necessarily exhaustive these locations should include all relaxation/meal areas, toilets, showers, change rooms and locker rooms.²⁸⁹

3.146 Surveillance in these private areas has a social impact that compromises the quality of life²⁹⁰ of workers in their workplaces and demeans us as a community. In this context, a prescriptive form of regulation is warranted.

3.147 Where an employer has previously used a form of surveillance in the places listed under the prohibition, it will need to devise other less invasive methods for meeting its requirements, assuming the measures are necessary at all. The draft Bill in Appendix 5 also provides that the prohibition may apply to other prescribed circumstances.

286 *Surveillance Devices Act 1999* (Vic) s 11, note exceptions in s 11(2).

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

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

289 Options Paper submission 28.

290 Department of Treasury and Finance (2005), above n 144, 5-11.



RECOMMENDATION(S)

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

OTHER LEGISLATION

SURVEILLANCE DEVICES ACT

3.148 The Surveillance Devices Act already places some limits on the use of optical and audio surveillance devices and tracking devices. As we have discussed, this Act has limited relevance to workers because most conversations or activities in the workplace do not come within the definition of private conversations or activities. In addition, workers who consent to surveillance are not protected. Our intention is that the Surveillance Devices Act's provisions should no longer apply to acts or practices which are used by employers in the context of employer-worker relationships. In other words, the workplace privacy legislation will comprehensively regulate practices that affect workplace privacy. The Surveillance Devices Act should be amended to make this clear.

LAW ENFORCEMENT

3.149 As is currently the case under the Surveillance Devices Act, the workplace privacy legislation is not intended to affect the powers which members of Victoria Police and other state and federal bodies exercise for law enforcement purposes,²⁹¹ and which are regulated by other legislative controls. For example, the proposed legislation is not intended to cover police video surveillance of a worker to detect criminal activity.²⁹²

3.150 There may be some situations in which the act or practice affecting a worker is being done by an employer which is also a law enforcement agency; Victoria Police are the obvious example. On the one hand, police could be seen as workers with rights to

291 See *Surveillance Devices Act 1992* (Vic) s 3 for definition of law enforcement officer.

292 Cf *Surveillance Devices Act 1999* (Vic) ss 5, 9, 10, 12, pt 4.

privacy protection. While police occupy a special position in society, they are entitled to protection of their human rights along with every other member of the community.²⁹³ On the other hand, they are law enforcement officers. In some cases these roles may overlap. For example, a decision may be made to place a police officer under surveillance because it is suspected the officer is involved in criminal activity.

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

3.152 Issues which are particularly relevant to police should be dealt with under specific legislation rather than under the workplace privacy legislation proposed in this report. The Victorian Privacy Commissioner has responsibility for, and considerable experience in, considering the balance to be struck between privacy protection and other public policy concerns. We would expect the government to consult with the Privacy Commissioner about how privacy issues relevant to the police should be dealt with.²⁹⁴

OTHER LEGISLATION

3.153 Some acts or practices regulated under our proposed legislation may be expressly permitted under other legislation. The commission has not attempted to identify all the statutory provisions which affect practices considered in this report. If the government establishes the regulatory regime we recommend, it should consult government agencies and statutory authorities to identify such provisions and determine whether they should be retained. For this reason, the draft Bill in Appendix 5 does not contain statutory exceptions to deal with powers contained in other legislation, but it may be necessary to include such exceptions.

293 Police officers occupy a different position than that expected within a standard employer–employee relationship. See *Police Regulation Act 1958* (Vic) s 11, which states, ‘Every constable shall have such powers and privileges and be liable to all such duties as any constable duly appointed now has or hereafter may have either by the common law or by virtue of an Act of Parliament now or hereafter to be in force in Victoria, and any member of the police force of a higher rank than a constable shall have all the powers and privileges of constable whether conferred by this Act or otherwise’.

294 The commission is aware that amendments to the Police Regulation Act are under consideration by the Victorian Government.

**RECOMMENDATION(S)**

31. Acts or practices of employers which involve installation, use or maintenance of surveillance devices in relation to their workers should be regulated by the Workplace Privacy Act. The Surveillance Devices Act should be amended accordingly.

32. The Department of Justice should consult with government agencies and statutory entities to determine whether statutory provisions in other legislation which affect workplace privacy should be repealed or retained.

Chapter 4

Promoting Compliance

INTRODUCTION

4.1 Chapter 3 sets out the central elements of the proposed workplace privacy legislation. This chapter makes recommendations which are intended to encourage employers to avoid unreasonable breaches of workers' privacy, to provide effective remedies to workers whose privacy has been unlawfully invaded, and to impose sanctions for non-compliance. Appendix 5 of this report includes a draft Workplace Privacy Bill. This chapter outlines the broad administrative framework which underpins the legislation but does not discuss all of the detail in the provisions contained in the draft Bill.

4.2 The sections in this chapter deal with:

- appointment of a statutory office to administer the workplace privacy legislation (in the following discussion this office and the person heading it are described as 'the regulator');
- the necessary characteristics and main functions of the regulator, which include promoting compliance with the legislation, dealing with systemic workplace privacy issues and handling complaints;
- how the regulator will hear and resolve complaints;
- how the obligations created by the legislation will be enforced;
- the jurisdiction of VCAT.

4.3 The legislative compliance framework proposed in the draft Bill is largely based on provisions in other human rights legislation—the Information Privacy Act, the Health Records Act, the Human Rights and Equal Opportunity Act, the Occupational Health and Safety Act and the Equal Opportunity Act. We have also taken account of submissions, comments made at roundtables, and issues raised in consultations with the Health Services Commissioner and the Victorian Privacy Commissioner.

STATUTORY OFFICE TO OVERSEE LEGISLATION

4.4 We recommend that a statutory officer be given responsibility for overseeing the operation of the proposed workplace privacy legislation.

4.5 The regulatory trend in Victoria, and elsewhere in Australia, has been to establish separate bodies to regulate different areas of human rights law, for example equal opportunity and privacy laws.

4.6 One employer perceived a regulator as offering a more informal, community-based approach to that offered by the traditional court process:

The court bases its recommendations on law. The regulator at least could in consultation with stakeholders come to some basic agreement on how applications are to be processed and the basics of what is acceptable or not. These would be based on general principles of community acceptability.²⁹⁵

4.7 The Victorian Privacy Commissioner is responsible for overseeing the Information Privacy Act, which establishes a regime for the handling of personal information in the Victorian public sector.²⁹⁶ The Health Services Commissioner is responsible for the Health Records Act, which imposes obligations on public and private organisations which hold health information.²⁹⁷ The Equal Opportunity Commission of Victoria (EOCV) oversees the Equal Opportunity Act, which establishes a regime to protect people from discrimination and promote equality of opportunity.²⁹⁸

4.8 In its submission, the EOCV raised concerns about a fragmented approach to the protection of human rights in Victoria²⁹⁹ and recommended, ‘...consideration should be given to making the regulation of workplace privacy the responsibility of the EOCV with advice from Victoria’s Privacy Commissioner’.³⁰⁰ The submission argued that this would build on existing expertise at the EOCV and allow protection of privacy to be addressed within a broader human rights framework.³⁰¹

295 Options Paper submission 23.

296 *Information Privacy Act 2000* (Vic) s 1 (purposes), s 50 (privacy commissioner).

297 *Health Records Act 2001* (Vic) ss 10, 11, 12.

298 *Equal Opportunity Act 1995* (Vic) s 1 (purposes), s 161 (functions and powers of commission).

299 Options Paper submission 26.

300 Ibid.

301 Options Paper submissions 26, 2.

4.9 We recognise that at some time in the future the government may wish to consider bringing together the various bodies which deal with human rights issues in Victoria under the umbrella of a generalist human rights body. There may be advantages in having one body to oversee the operation of human rights legislation. At this stage, however, we do not support the approach proposed by the EOCV. While anti-discrimination laws and privacy laws are both designed to protect human rights, the legal issues involved are different and specialist expertise is required to deal with them. The EOCV proposal addresses only workplace privacy issues and does not deal with the other aspects of privacy which are currently regulated by the Information Privacy Act and the Health Records Act. As a result, the EOCV proposal would not address the fragmentation it criticises.

4.10 The Privacy Commissioner deals with the privacy of personal information held by government agencies and the Health Services Commissioner deals with the privacy of health records. There will often be a close relationship between practices which affect privacy (eg surveillance) and the personal information that may be collected as a result of these practices. It would be confusing for members of the community to have to deal with another statutory body with responsibility for promoting privacy in the workplace. The commission therefore believes that, at present, the Privacy Commissioner may be the most appropriate body to administer the workplace privacy legislation.

4.11 Nonetheless, we have not made a formal recommendation to this effect because of other discussions about human rights protection currently underway in Victoria. These include a community consultation on the introduction of a Charter of Rights and possible changes to the Equal Opportunity Act which were proposed in the Attorney-General's Justice Statement.³⁰²

REGULATOR CHARACTERISTICS

INDEPENDENCE

4.12 The workplace privacy regulator will have responsibility for overseeing both public and private sector compliance with the legislation. It is important that the role of the regulator should not be politicised and that the regulator should be, and should be seen to be, acting independently of government in exercising the functions

302 See Department of Justice, *New Directions for the Victorian Justice System 2004–2014: Attorney-General's Justice Statement* (2004) 52–57; Human Rights Consultative Committee, *Have Your Say About Human Rights in Victoria: Human Rights Consultation Community Discussion Paper* (2005).

conferred by the Act. Because the regulator will have to handle complaints from public sector employees, the government should not be able to direct the way the regulator exercises its powers. Ensuring the regulator's statutory functions are exercisable without political interference will also be important in building employers' and workers' confidence in the fairness of the scheme.

4.13 The Public Accounts and Estimates Committee recently reported on corporate governance in the Victorian public sector.³⁰³ The report referred to the factors which determine whether a statutory body is, and is seen to be, independent from government departments. These factors include how the regulator is appointed and the basis on which he or she can be removed, whether the regulator appoints his or her own staff, to whom the regulator reports and how the office is funded.³⁰⁴

4.14 The commission recommends that the regulator be appointed for a specified term by the Governor in Council and should not be removed during this term unless convicted of a criminal offence, or he or she becomes incapable because of physical or mental incapacity.³⁰⁵ The regulator's office should be a 'special body' under section 6 of the Public Administration Act³⁰⁶ and the regulator should have the functions of a public service body head in relation to staff.³⁰⁷

ACCOUNTABILITY AND TRANSPARENCY

4.15 Reporting requirements will help to make the regulator accountable to the public and ensure its powers are exercised transparently. Reports can also be used to educate employers and workers about the legislation and their obligations and responsibilities under it.

4.16 The Victorian Privacy Commissioner may, in the public interest, publish reports and recommendations and report to the relevant government minister on any act or practice that the commissioner considers breaches an individual's privacy. The

303 Public Accounts and Estimates Committee, *Report on the Inquiry into Corporate Governance in the Victorian Public Sector*, 63rd Report to the Parliament (May 2005) 174.

304 See also Fiona Smith, 'Independence and Governance: One Perspective' (Paper delivered at Statutory Entities Forum, Melbourne, 20 July 2005).

305 Cf *Information Privacy Act 2000* (Vic) s 53, which also includes insolvency as a basis for removal.

306 Special bodies are those which require a high degree of independence from the executive and include the office of the Health Services Commissioner, the office of the Privacy Commissioner, the office of the Ombudsman, and the Victorian Auditor-General's office. See Peter Harmsworth, 'State Services Authority Overview' (Paper delivered at Statutory Entities Forum, Melbourne, 20 July 2005).

307 *Public Administration Act 2004* (Vic) ss 6, 16.

minister may table that report in parliament.³⁰⁸ We propose a similar power be conferred on the workplace privacy regulator. To ensure the regulator is accountable to the public, as well as to the relevant government minister, we recommend that the minister be required to table these reports in parliament. We also recommend that the annual reporting obligations imposed by section 43 of the *Financial Management Act 1994* apply to the regulator. This Act requires reports of operations and audited financial statements of public bodies to be laid before each House of Parliament.³⁰⁹ The annual report may be a valuable source of information about the practices occurring in particular workplaces. The regulator should be required to report on the number of authorisations granted to employers to use acts or practices which affect the privacy of workers when they are not working, as well as authorisations granted for genetic testing.

4.17 In paragraphs 4.94–4.100 we recommend that VCAT have jurisdiction to hear issues arising from privacy complaints and review various decisions made by the regulator. These provisions will contribute to the consistency and accuracy of the regulator’s decisions and are another means of ensuring regulator accountability.

EXPERTISE

4.18 The regulator should have expertise in privacy law and practice and human rights law. Because of the overlap which may occur between privacy and industrial relations issues, it would also be desirable for the regulator to have some knowledge of industrial relations.



RECOMMENDATION(S)

33. A statutory office of the workplace privacy regulator should be established.
34. The workplace privacy regulator should be appointed by the Governor in Council for a term not exceeding seven years and should only be able to be removed from office for misbehaviour or incapacity.

308 *Information Privacy Act 2000* (Vic) s 63.

309 *Financial Management Act 1994* (Vic) s 46.

! RECOMMENDATION(S)

35. The office of the workplace privacy regulator should be a 'special body' and the workplace privacy regulator should have the functions of an agency head in relation to employees according to the *Public Administration Act 2004*.
36. The workplace privacy regulator should be required to report annually to parliament.
37. The workplace privacy regulator should also have the power to report to the relevant minister on matters relating to his or her functions under the workplace privacy legislation. The minister should be required to table these reports in parliament.

REGULATOR FUNCTIONS

4.19 The regulator will have responsibility for overseeing the operation of the workplace privacy legislation. We recommend that the workplace privacy regulator have similar functions to those exercised by the Privacy Commissioner and the Health Services Commissioner. The following sections discuss the main functions of the regulator. These include:

- promoting understanding of and compliance with the legislation;
- preparing advisory and mandatory codes of practice;
- authorising acts or practices which affect the privacy of workers involved in non-work-related activities and genetic testing;
- dealing with systemic acts or practices which may have an effect on workers' privacy;
- making recommendations to the minister about existing or proposed legislation which may have adverse effects on workers' privacy;
- receiving and resolving complaints about acts or practices which may not comply with the scheme.

Some of these functions, such as the preparation of advisory and mandatory codes of practice and the granting of authorisations, have already been discussed. The other proposed functions are discussed below.

PROMOTING COMPLIANCE THROUGH EDUCATION

4.20 One of the main roles of the regulator will be to promote understanding of and compliance with the legislation. Education of employers and workers will ensure they understand their rights and responsibilities under the legislation.³¹⁰ Education is an essential non-legislative measure to ensure compliance with statutory obligations³¹¹ and its importance has been acknowledged on many occasions. For example, the former federal Privacy Commissioner has commented that, 'Promotion and education are key tools used by the Office in meeting our responsibility to encourage adoption of privacy standards more broadly in the community'.³¹²

4.21 Submissions to the Options Paper pointed to areas such as occupational health and safety and equal opportunity, where education on legal rights and responsibilities has helped to change employer and worker behaviour in the workplace.³¹³ Participants in our roundtables agreed that education of employers and workers about workplace privacy could assist in bringing about cultural change at an organisational level.³¹⁴ One roundtable participant suggested 'mandatory education' form part of the regulator's powers. Another participant made the useful suggestion that the regulator create networks with relevant third parties (eg the Australian Psychological Society, the Biometrics Institute (Australia) and surveillance and monitoring technology providers) so they too could form an integral part of the educative process.³¹⁵

4.22 Education was also seen as an important way to smooth the path into a new regulatory scheme. One employer suggested that any new regime should incorporate an educative period before the new regulation took effect.³¹⁶

4.23 Both the Information Privacy Act and the Health Records Act give their commissioners the function of promoting understanding and acceptance of relevant privacy principles. The commission recommends that the workplace privacy regulator

310 The importance of education was acknowledged in Office of the Privacy Commissioner, *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (2005) 108–109. See also Office of the Victorian Privacy Commissioner, *Annual Report 2003–04* (2004) 8–19.

311 Department of Treasury and Finance (2005), above n 144, 1–7.

312 Office of the Privacy Commissioner [Aus], *The Operation of the Privacy Act Annual Report, 1 July 2000–30 June 2001* (2001) 44.

313 Options Paper submissions 8, 9, 24.

314 Roundtable 3.

315 Roundtable 1.

316 Roundtable 3. See also roundtable 5.

have a similar function. Provision of advice on steps that need to be taken to comply with the legislation will also serve this function. We recommend that the regulator be able to respond to queries and advise employers and workers about compliance.³¹⁷

RESOLVING COMPLAINTS

4.24 In the Options Paper, the commission proposed that workers who believe their privacy has been breached by their employer should be able to complain to the regulator. Many stakeholders were in favour of including a complaints process in a regulatory scheme and recognised the importance of providing a cheap, informal and flexible method of resolving disputes.³¹⁸ Some stakeholders also commented that workers are well placed to be able to identify where breaches are occurring and to communicate that information to a regulator.³¹⁹

4.25 Incorporating a complaints-based mechanism into the workplace privacy regime is consistent with existing federal and state privacy laws and with other legislative regimes which protect human rights.³²⁰ The commission recommends that the regulator have the power to receive, conciliate, investigate and make rulings on complaints. In the course of dealing with complaints, the regulator will be able to require an employer to attend and give evidence or produce information and documents, and to audit and monitor acts or practices of the employer to determine whether it is complying with the legislation. The complaints–resolution process is discussed in more detail in paragraphs 4.46–4.72.

4.26 As we discuss in the next section, a complaints–resolution process which focuses on the grievances of particular individuals will not necessarily result in long-term cultural changes which ensure appropriate respect for workers' privacy. To deal with this issue, it is important for the regulator to have powers to identify workplace privacy problems which extend beyond particular complaints and take steps to bring about systemic changes.

317 The Victorian Privacy Commissioner has a similar function: *Information Privacy Act 2000* (Vic) s 58(s); and see Office of the Victorian Privacy Commissioner (2004), above n 310, 21.

318 See, eg, Options Paper submission 22; roundtable 3, in which one participant commented that as privacy means different things to different people, it is important to have a flexible dispute resolution system that caters for these differences.

319 Roundtable 3.

320 Eg, there are complaints-based systems incorporated in the *Equal Opportunity Act 1995* (Vic) pt 7; *Information Privacy Act 2000* (Vic) pt 5; *Health Records Act 2001* (Vic) pt 6; *Privacy Act 1988* (Cth) pt V, div 1.

WHY A SYSTEMIC APPROACH IS NECESSARY

4.27 The commission believes the proposed regime will only provide adequate privacy protection if the regulator is able to go beyond dealing with individual complaints to take a more systemic approach to workplace privacy issues. Although human rights legislation has traditionally relied on complaints to identify breaches and provide remedies to individuals who are affected, there is increasing recognition that this reactive approach does not prevent breaches occurring and may not deal effectively with broader problems in particular workplaces or industries. In the context of discrimination, the EOCV has commented on the difficulties of dealing with human rights breaches on a case-by-case basis:

Few people act on their right to complain about discrimination due to their fear of retribution or being marginalised in their social or work networks. Complainants bear the onus, cost and emotional stress of initiating and driving complaints.³²¹

4.28 The Attorney-General's Justice Statement suggested that greater protection of human rights could be achieved by 'moving the focus of the Equal Opportunity Act away from responding to complaints towards proactive and creative forms of compliance'.³²²

4.29 Similar problems arise in the context of workplace privacy. Workers may be reluctant to complain about employer acts which unreasonably breach their privacy because their employment is precarious or their livelihood is threatened.³²³ An employer may pressure workers to agree to practices which do not comply with the legislation.³²⁴ Roundtable participants commented that it was a 'brave individual' who took on an employer when there was an ongoing work relationship—particularly in smaller or non-unionised workplaces.³²⁵ Job applicants are particularly unlikely to complain about acts or practices of a prospective employer which affect their privacy.

4.30 Regulatory theorists have also argued that emphasis on resolving individual complaints has limited effect when breaches are a necessary consequence of corporate

321 This was reported in Department of Justice (2004), above n 302, 56–57.

322 Ibid 57.

323 Issues Paper submission 22.

324 For discussion of the power imbalance which may make it difficult for employees to object to particular practices see Caroline Morris, 'Drugs, the Law, and Technology: Posing Some Problems in the Workplace' (2002) 20 *New Zealand Universities Law Review* 1, 27. See also the discussion in Issues Paper submission 1; VLRC (September 2004), above n 16, paras 3.60–3.68.

325 Roundtable 5.

systems or operations.³²⁶ The complaints–resolution process may address a problem experienced by an individual but will not necessarily result in the employer making changes to systems. For example, an employer might use a GPS system to track workers’ movements after hours. If an individual worker complains, conciliation of the complaint could address the particular worker’s concern but would not necessarily prevent other workers being tracked out-of-hours. By contrast, if the regulator undertook a broader investigation of GPS tracking used by that employer, changes could be made to benefit all those who worked there. From a regulatory perspective, solutions would be preventative rather than reactive in nature.

4.31 Both public and industry-based complaints-handling schemes have recognised that dealing with individual complaints has limited capacity to bring about changes, and so have introduced systemic complaints-handling processes.³²⁷ In the Victorian public sector, the Office of the Ombudsman has the power to conduct an investigation without receiving a complaint.³²⁸ In the private sector, the Banking and Financial Services Ombudsman identifies and reports systemic problems to the Australian Securities and Investment Commission.³²⁹ Similarly, the Telecommunications Industry Ombudsman introduced a systemic complaints procedure in February 2002.³³⁰

4.32 We recommend that the regulator have the power to undertake two different kinds of systemic investigation:

- conducting an investigation which extends beyond the terms of a particular complaint;
- undertaking an inquiry into acts or practices which affect workers’ privacy.

326 Brent Fisse and John Braithwaite, *The Impact of Publicity on Corporate Offenders* (1983) 57.

327 National Alternative Dispute Resolution Advisory Council, ‘Resolving Customer Disputes: Case Studies and Current Issues’ (Panel discussion at the ADR—A Better Way to do Business conference, Sydney, 4–5 September 2003) <www.ag.gov.au> at 8 August 2005.

328 *Ombudsman Act 1973* (Vic) s 14.

329 See Australian Securities and Investment Commission, *Approval of External Complaints Resolution Schemes*, Policy Statement 139 (1999) pursuant to Corporations Regulation 7.3.02B to the *Corporations Act 2001* (Cth).

330 See *Policies and Procedures: 18.5 Systemic Issues Complaints*, Telecommunications Industry Ombudsman <www.tio.com.au/POLICIES/complaint%20escalation.htm#185> at 16 August 2005.

The regulator's capacity to receive complaints made by an individual, or a body representing a number of individuals, will also allow the regulator to consider systemic privacy breaches, as we discuss in the next section.

GOING BEYOND THE TERMS OF A PARTICULAR COMPLAINT

4.33 The Equal Opportunity Act allows the EOCV to conduct an investigation while dealing with a complaint in order to deal with matters other than the subject of the complaint.³³¹

4.34 The commission recommends that the regulator have similar power to conduct an investigation of matters other than the breach which is the subject of a complaint. For example, while handling a complaint about inappropriate use of overt surveillance in the workplace, the regulator might be told workers were being subjected to surveillance outside work. Clause 61 of the draft Bill will give the regulator power to investigate this matter, attempt to resolve it or make a binding ruling on it. In carrying out this investigation, the regulator will have similar powers to those which apply in investigating a complaint, including the power to require a person to give evidence or produce documents and the power to undertake audits and monitor the use of equipment.

UNDERTAKING AN INQUIRY

4.35 With the approval of the minister, the Health Services Commissioner can initiate inquiries into matters referred to it by the Health Services Review Council and 'broader issues of health care arising out of complaints'.³³² We recommend that in addition to the regulator's power to investigate breaches which come to its notice while handling complaints, it should also be able to conduct inquiries and publish reports on issues relating to workplace privacy.

4.36 If an issue comes to the regulator's attention as a result of a complaint or because of research undertaken, this power would enable the regulator to consider the matter and consult with experts and the community to identify the nature and extent of the problem. The Victorian Trades Hall Council supported the regulator initiating inquiries:

331 *Equal Opportunity Act 1995* (Vic) s 156(3).

332 *Health Records Act 2001* (Vic) s 87(g).

Issues of consent and the unequal nature of the contract between workers and employers requires the involvement of a party independent of the contract and [sic] be able to present material which otherwise might be prejudicial to the future prospects of an individual worker or group of workers.³³³

4.37 In paragraphs 4.12–4.14 we recommended the regulator’s powers be exercised independently of the political process. For this reason, we do not see any basis for requiring ministerial approval before an inquiry is undertaken and do not propose this requirement should apply.

4.38 The commission believes the use of an inquiry power will enable the regulator to provide advice to employers, or take other measures, before a practice which affects workers’ privacy has become widespread.

INQUIRY PROCESS

4.39 Our proposed process of inquiry is based largely on the existing federal Human Rights and Equal Opportunity inquiry process.³³⁴ We propose that the regulator be able to conduct an inquiry in any manner it sees fit, and inform itself without being bound by the rules of evidence.³³⁵ The regulator should be able to engage in consultations with individuals and organisations and allow members of the public to make submissions. In exercising its inquiry powers, it is recommended the regulator be empowered to require production of documents and to examine witnesses.³³⁶

POSSIBLE INQUIRY OUTCOMES

4.40 The inquiry power is intended to allow the regulator to focus on systemic issues, such as the use of a particular practice by employers or the use of acts or practices within a particular industry. An inquiry may reveal breaches of the legislation by particular employers but its primary purpose will be to identify systemic workplace privacy problems and guide the development of policy to deal with them.

333 Options Paper submission 28.

334 *Human Rights and Equal Opportunity Act 1986* (Cth) ss 11, 14, 20, 21, 24, 26–30, 32–5.

335 For a similar provision see *Health Records Act 2001* (Vic) s 68.

336 Witnesses who provide evidence to the regulator should be immune from defamation as is provided for in, eg, *Equal Opportunity Act 1995* (Vic) s 210.

4.41 At the conclusion of an inquiry, the regulator will be required to report to the minister. The minister will be required to table the report in parliament.

4.42 The regulator will also be able to exercise various powers based on findings in the inquiry. For instance, the regulator might exercise its power to issue advisory codes of practice as a result of its findings. The regulator could also recommend changes to the Act or recommend particular acts or practices require authorisation or be regulated by mandatory codes. The regulator may decide an education program is the most appropriate way of resolving issues raised by its findings.

FUNDING A SYSTEMIC APPROACH

4.43 Those who supported the regulator having power to deal with systemic issues³³⁷ said it would be ineffective unless the regulator was adequately funded.³³⁸ It was pointed out that similar powers conferred on bodies such as the federal Human Rights and Equal Opportunity Commission were not used, or only used ‘once in a blue moon’.³³⁹

4.44 We have emphasised the importance of educating employers and workers about their rights and obligations under the legislation. In appropriate cases, the regulator’s power to deal with systemic issues may also help to identify problems and assist employers to resolve them. The commission does not usually make recommendations in relation to resources. However, we acknowledge that the exercise of these functions will require an appropriate level of funding.

ADVISING GOVERNMENT ON WORKPLACE PRIVACY

4.45 Various legislative provisions may affect workers’ privacy. For example, legislation could be enacted to require workers in particular industries to have regular drug and alcohol tests or to provide information about their financial affairs to their employer. The regulator should play a role in advising the government on legislation or practices that affect workers’ privacy. The Victorian Privacy Commissioner currently performs a similar function in relation to government practices or laws that affect information privacy.³⁴⁰ It would be useful for the regulator and the government

337 Roundtable 5.

338 Roundtables 1, 5.

339 Roundtables 1, 5.

340 *Information Privacy Act 2000* (Vic) s 58(c); Office of the Victorian Privacy Commissioner (2004), above n 310, 29–34.

to reach an agreement about the practical issues which will arise in exercising this function (eg about the process for obtaining the regulator's views on proposed legislation before Cabinet gives approval in principle to a proposal). Subject to the processes governing the preparation of legislation, the regulator's comments should be made publicly available.

! RECOMMENDATION(S)

38. The main functions of the workplace privacy regulator are to:

- promote understanding of and compliance with the workplace privacy regime;
- provide educational programs to promote understanding of the workplace privacy regime;
- provide advice to any person or organisation on compliance with the legislation;
- issue guidelines on the development of approved codes of practice prepared by employers or groups of employers;
- receive complaints about an act or practice of an organisation that may contravene the workplace privacy legislation and investigate, conciliate and make rulings on complaints;
- conduct audits of acts or practices of an employer to ascertain whether the employer is complying with obligations under the workplace privacy legislation;
- monitor and report on the adequacy of equipment and system safeguards put in place to minimise the effect of acts or practices on workers' privacy;
- conduct an investigation beyond the terms of a particular complaint;
- conduct an inquiry into acts or practices which affect workers' privacy;
- assess any proposed or existing legislation that may adversely affect the privacy of workers or otherwise contravene the provisions of the Act, including reporting to the minister the results of the assessment;

! RECOMMENDATION(S)

- make public statements in relation to any matter affecting workplace privacy;
 - undertake research into and monitor developments affecting workplace privacy.
39. The regulator should have the power to investigate acts or practices of an employer which come to the regulator's attention while dealing with a complaint, in order to deal with privacy breaches of the same or a different kind as the breach which is the subject matter of the complaint.
40. In exercising the function to conduct an inquiry, the regulator should have the power to obtain information and documents and examine witnesses.
41. In exercising the function to audit and monitor, the regulator should have the power to obtain information and documents, examine witnesses and to enter premises.

INDIVIDUAL COMPLAINTS—RESOLUTION PROCESS

4.46 In the previous section, we referred to the regulator's function of receiving and resolving complaints. In this section, we provide an outline of the proposed individual complaints—resolution process, which is similar to those under the Information Privacy Act and Health Records Act.³⁴¹ The following sections cover:

- who should be able to complain;
- initial assessment of the complaint;
- the regulator's power to decline a complaint;
- the regulator's powers if a complaint is accepted.

Further details of the complaints process are contained in the draft Bill in Appendix 5.

341 *Information Privacy Act 2000* (Vic) pt 5; *Health Records Act 2001* (Vic) pt 6.

WHO SHOULD BE ABLE TO COMPLAIN

4.47 Complaints will usually be made by individuals. Under the Health Records and Information Privacy Acts, however, where an act or practice breaches the privacy of two or more people, any one of those people can complain on behalf of all of the individuals who consent to the complaint being made.³⁴² We recommend that a similar provision be included in the workplace privacy legislation.

4.48 Some stakeholders also thought that a union or other organisation should be able to make a complaint as a representative of an affected worker.³⁴³ This may be appropriate where a number of workers are affected by an act or practice which breaches their privacy and/or where individuals are reluctant to complain because of concerns their employment may be affected.

4.49 The *Racial and Religious Tolerance Act 2001* allows complaints to be made by a representative body on behalf of individuals where the representative body has sufficient interest in the complaint because the conduct adversely affects the interests of the body or the persons it represents.³⁴⁴ The commission recommends that the workplace privacy legislation make similar provision for representative complaints. As well as trade unions, other organisations such as professional associations could act as representatives of affected workers.

4.50 In paragraph 2.44 we refer to employers' concerns that a privacy complaint could provide the basis for larger industrial disputes. Provision for union representation may be seen as increasing the likelihood this will occur. In some situations it may be preferable for complaints about privacy invasions to be dealt with as an industrial relations matter. Recommendation 48 therefore permits the regulator to decline a complaint where it can be dealt with more appropriately in another forum.

INITIAL ASSESSMENT OF THE COMPLAINT

4.51 When the regulator receives a complaint, it will make an initial assessment of it to determine the course of action to take. We recommend that the regulator have the power to require any relevant documents to be produced, to require any person to attend before the regulator or to require a written initial response to the complaint

342 *Information Privacy Act 2000* (Vic) s 25(3); *Health Records Act 2001* (Vic) s 45(3).

343 Roundtable 4; Options Paper submission 28.

344 *Racial and Religious Tolerance Act 2001* (Vic) s 19.

from the employer.³⁴⁵ The regulator should have the power to deal with the matter informally. This may be appropriate where the employer admits that an unintentional or minor breach has occurred and agrees to rectify it.³⁴⁶ Such a provision recognises the minor or unintentional nature of such breaches and allows for the regulatory impact to be minimised.

REGULATOR'S POWER TO DECLINE THE COMPLAINT

4.52 Employer organisations expressed various concerns about complaints processes. One employer was concerned about the problem of serial or frivolous complainants and about the cost which might be incurred by employers in handling complaints.³⁴⁷ To meet concerns about unmeritorious complaints, we recommend that the regulator be able to decline a complaint if:

- there is no evidence of a breach of the individual's privacy which is a breach of the workplace privacy legislation;
- the complaint is made more than 12 months after the incident or last incident occurred);³⁴⁸
- the complaint is frivolous, vexatious, misconceived or lacking in substance.

4.53 Some privacy complaints raise broader industrial relations issues. For example, workers might complain to the regulator about intensive use of video surveillance to increase productivity. Employers argued that these issues are better dealt with as industrial relations disputes than as privacy complaints.

4.54 There are also situations where a complainant may have a remedy under other legislation. For example, the employer may have breached workers' privacy and also discriminated against them on grounds which are prohibited by the Equal Opportunity Act.

4.55 To deal with these situations, we recommend that the regulator be able to decline a complaint if the act or practice:

345 This is the way complaints are handled by the Equal Opportunity Commission of Victoria, with the exception of requiring people to attend before the commission.

346 Cf *Health Records Act 2001* (Vic) s 49(3).

347 Roundtable 3.

348 The regulator has discretion to extend this timeframe—see clause 37(7) of the draft Bill contained in Appendix 5.

- has been the subject of an application under other legislation or a proceeding in a court or tribunal and has been adequately dealt with by these other means;³⁴⁹
- is the subject of an application under other legislation or a proceeding in a court or tribunal and is being adequately dealt with by these other means;
- could be made the subject of an application to another forum which would, in the opinion of the regulator, be more appropriate.³⁵⁰

4.56 Regulatory theorists at our roundtables encouraged the idea that the regulator should establish links with regulators in other jurisdictions to ensure the complaint is heard in the most appropriate jurisdiction.³⁵¹ Such interaction creates the added benefit of regulators becoming aware of developments in other related jurisdictions.

4.57 Some employers may decide to set up an internal complaint-handling process. Such a process could be included in a code of practice prepared by the employer and approved by the regulator. We therefore recommend that the regulator be able to decline a complaint if it has been made to the respondent and the respondent is dealing with it under a process set up under an approved code of practice, or is otherwise dealing adequately with it. Similar powers to decline complaints are contained in the Information Privacy Act and the Health Records Act.³⁵²

4.58 The regulator will be required to notify the complainant and respondent if the complaint is declined on one of the grounds discussed above. As is the case under the Information Privacy Records Act and the Health Records Act, the complainant will then be able to require the regulator to refer the matter to VCAT for a hearing. The role of VCAT is discussed in paragraphs 4.94–4.100 below.

REGULATOR'S POWERS IF COMPLAINT IS ACCEPTED

CONCILIATION

4.59 In the Options Paper, we proposed the regulator should be able to deal with complaints by conciliating them, investigating them or a combination of both techniques. A number of submissions which commented on this issue said both

349 Cf *Equal Opportunity Act 1995* (Vic) s 108(1)(ba).

350 Cf *Equal Opportunity Act 1995* (Vic) s 108(1)(b).

351 Roundtable 1.

352 See *Information Privacy Act 2000* (Vic) s 29; *Health Records Act 2001* (Vic) s 51.

conciliation and investigation should be available and the regulator should be able to decide which was appropriate in the circumstances.³⁵³

4.60 The Health Services Commissioner treats conciliation as the main method of resolving complaints about health services, including disputes about health records.³⁵⁴ Similarly, the Victorian Privacy Commissioner has commented that, 'Victoria's information privacy scheme stresses conciliation, which is especially appropriate in privacy matters because they tend to be inherently delicate'.³⁵⁵

4.61 The commission believes there are many advantages in conciliating complaints about workplace privacy issues. As one submission pointed out, conciliation will often be the preferred method because it is cost-effective, less likely to spark employee or union resistance and emphasises cooperation rather than confrontation.³⁵⁶ It may also prevent exposure of material which the worker wishes to keep confidential. Conciliation may also help to bring about changes in acts or practices which have the potential to affect workers' privacy. Where the regulator declines to conciliate or conciliation fails, the complainant will be able to request that the matter be referred to VCAT.

4.62 In some situations, the regulator may consider it inappropriate to attempt to conciliate a complaint. We recommend below that the regulator should have the power to investigate the complaint and make a ruling.

INVESTIGATION AND RULING

4.63 Under the Health Records Act, the Health Services Commissioner has the power to investigate a complaint and make a ruling on whether the act or practice which is the subject of the complaint is a breach of the privacy of the complainant.³⁵⁷

4.64 The commission recommends that the regulator under the workplace privacy legislation also be able to investigate a complaint and make a ruling on it. Investigation and/or a ruling may be appropriate where a party refuses to conciliate, where there is a systemic problem in a particular workplace, and/or where the regulator considers the

353 Options Paper submissions 4, 5, 9, 16.

354 Health Services Commissioner, *Annual Report* (2004) 18.

355 Office of the Victorian Privacy Commissioner (2004), above n 310, 3.

356 Options Paper submission 24.

357 *Health Records Act 2001* (Vic) s 64.

worker would be at a significant disadvantage in the conciliation process.³⁵⁸ The ruling may identify any action which is required to remedy the breach of privacy. Both parties have the right to object to the ruling and have the matter referred to VCAT.³⁵⁹ Recommendation 50 specifies the matters which may be included in a ruling.

4.65 As is the case under the Health Records Act,³⁶⁰ the respondent should be required within a specified period to report to the regulator on the action taken with respect to a ruling. If the respondent does not seek a VCAT hearing in relation to the ruling, and does not comply with the ruling, we recommend that the complainant be able to register a copy of the ruling signed by the regulator with VCAT. Once it is registered, the ruling should be treated as if it were an order of VCAT and be enforceable in the same way. VCAT orders that are not complied with can be filed in the appropriate court and are then enforceable as if they are court orders.³⁶¹

4.66 The recommended procedure for registering the regulator's ruling in VCAT differs from the procedure under the Health Records Act. Under that Act, if the respondent does not comply with a ruling of the Health Services Commissioner a complainant who wishes to enforce it must require the Health Services Commissioner to refer the matter to VCAT for a hearing. If VCAT makes a finding, it is then enforceable in the same way as other VCAT orders.³⁶²

4.67 We believe this process makes it very difficult for a complainant to obtain a remedy against a non-complying respondent. Even after the complainant has satisfied the regulator that a ruling should be made, the complainant is then forced to repeat the process before the tribunal. Under our recommendation, the respondent's right to contest the ruling before VCAT is preserved, but if he or she fails to do so, the registered ruling is enforceable by VCAT.

358 Concerns about worker disadvantage were expressed in Options Paper submission 23. Options Paper submission 4 also suggested that investigation may be useful in situations where workers feel there has been a significant breach of their privacy.

359 For discussion of the powers of VCAT see paras 4.94–4.100.

360 *Health Records Act 2001* (Vic) s 64.

361 *Victorian Civil and Administrative Tribunal Act 1998* (Vic) s 121 (enforcement of monetary orders), s 122 (enforcement of other orders by filing in the Supreme Court). No filing fee is payable.

362 *Health Records Act 2001* (Vic) s 65 (2), and see n 361.

4.68 The provision for registration at VCAT is similar to the process provided for enforcement of conciliation agreements under the Health Records Act and the Equal Opportunity Act.³⁶³

RULINGS AFFECTING THIRD PARTIES

4.69 Where the regulator is satisfied that the act or practice affects people other than the complainant, the regulator should be able to make a ruling to protect the privacy of people other than the complainant.³⁶⁴

POWERS NECESSARY FOR INVESTIGATION AND RULING

4.70 We recommend that the regulator be able to require a person to attend and answer questions or to produce documents while it is investigating a complaint. In addition, the regulator should be able to exercise the auditing and monitoring functions proposed by Recommendation 38. To determine whether a complaint can be substantiated, the regulator will be able to:

- audit records kept by employers to ascertain whether the information collected through acts or practices affecting workplace privacy is being used for the purposes for which it was collected;
- monitor and report on the adequacy of equipment and user safeguards, for example, software systems which record email use or the movements of workers tracked by a GPS device.

4.71 Both the Information Privacy Act and the Health Records Act have similar functions. For example, the Victorian Privacy Commissioner can ‘conduct and commission audits of records of personal information’ to ascertain whether they are being maintained in accordance with information privacy principles and can monitor and report on the adequacy of equipment and user safeguards. The Health Services Commissioner has similar functions in relation to health information.³⁶⁵

SEPARATING REGULATOR’S CONCILIATION AND INVESTIGATION FUNCTIONS

4.72 During roundtables, some participants expressed concerns about the potential for conflict between the regulator’s conciliation and investigation functions. Administrative separation of investigative and conciliation functions in the regulator’s

363 *Health Records Act 2001* (Vic) s 61; *Equal Opportunity Act 1995* (Vic) s 115.

364 A similar order is contained in recent amendments to the *Anti-Discrimination Act 1977* (NSW) s 108(3).

365 *Information Privacy Act 2000* (Vic) s 58(j)(k) and see also *Health Records Act 2001* (Vic) s 87(h)(i).

office should be used to deal with this issue. Along similar lines, conciliation by the Health Services Commissioner is ‘quarantined from the other work of the office; [proceedings] are confidential and privileged’.³⁶⁶

! RECOMMENDATION(S)

42. A worker or prospective worker should be able to complain to the regulator about an act or practice that may be a breach of the legislation.
43. Where an act or practice breaches the privacy of two or more workers, any one of them should be able to complain to the regulator on behalf of all workers who are affected, with their consent.
44. A representative body should be able to complain to the regulator on behalf of a worker or workers if that body has sufficient interest in the complaint.
45. A representative body should be regarded as having sufficient interest in the complaint if the conduct is a matter of concern to the body because of its effect on the interests of the body or the privacy of the person it represents.
46. The regulator should have the power to receive complaints about possible breaches of the legislation and to decline or accept them.
47. If the regulator decides to accept a complaint it may attempt to resolve it informally.
48. The regulator may decline a complaint if:
 - the act or practice about which the complaint has been made is not a breach of the individual’s privacy;

366 Beth Wilson, ‘Health Disputes: a “Window of Opportunity” to Improve Health Services’ in Ian Freckelton and Kerry Petersen (eds) *Controversies in Health Law* (1999) 185.

**RECOMMENDATION(S)**

- the complaint is made on behalf of a complainant by a person not authorised to do so;
- the complaint to the regulator was made more than 12 months after the complainant became aware of the act or practice;
- the complaint is frivolous, vexatious, misconceived or lacking in substance;
- the act or practice is the subject of
 - (i) an application under another enactment; or
 - (ii) a proceeding in a court or tribunaland the subject-matter of the complaint has been, or is being, dealt with adequately by that means;
- the act or practice which is the subject of the complaint could be more appropriately dealt with under another enactment;
- the act or practice is subject to an applicable code of practice or authorisation and mechanisms available for seeking redress under that code or authorisation have not been exhausted;
- the complainant has complained to the respondent about the act or practice and either
 - (i) the respondent has dealt, or is dealing, adequately with the complaint; or
 - (ii) the respondent has not yet had an adequate opportunity to deal with the complaint.

49. If the complaint is accepted the regulator may:

- attempt to resolve the matter informally;
- conciliate the complaint if appropriate;
- investigate the complaint and, if appropriate, make a ruling as to whether there has been a breach of privacy and set out any action which the regulator requires the employer to undertake to remedy the complaint.

! RECOMMENDATION(S)

50. A ruling may provide that:

- the employer must not repeat or continue the conduct;
- the employer must perform any reasonable act or undertake a course of conduct to redress any loss or damage suffered by the worker;
- any existing authorisation the employer possesses be revoked, or revoked until the employer takes specified action;
- the employer publish, at the employer's expense, an advertisement as specified in the order (the regulator may also publish details of the employer's conduct and/or number of complaints in its annual report).

51. Where the act or practice affects people other than the person making the complaint, the regulator may make a ruling to protect the privacy of people other than the person making the complaint, if having regard to the circumstances it is appropriate to do so.

52. If the respondent fails to comply with a ruling and does not seek to refer the matter to VCAT for hearing, the complainant can register the ruling with VCAT. On registration, the ruling is to be taken as an order of VCAT and can be enforced accordingly.

PROTECTING WORKERS AGAINST VICTIMISATION

4.73 One of the limitations of complaints-based systems is that people who have experienced a particular harm may be reluctant to complain because they fear victimisation. The Options Paper³⁶⁷ referred to a submission by the EOCV which commented that many victims of discrimination, harassment and vilification suffer from victimisation as a result of lodging a complaint.³⁶⁸ Concerns were also expressed

367 VLRC (September 2004), above n 16, para 4.83.

368 Ibid.

by roundtable participants about the potential for victimisation of workers who complained about a particular breach of privacy.³⁶⁹

4.74 Our recommendation that a representative body should be able to complain on behalf of a worker or group of workers will provide some protection against victimisation. We also recommend that the legislation specifically prohibit victimisation. If an employer retaliates, or threatens to retaliate, against a worker (including prospective workers) who has made a complaint or taken other action under the Act, the worker will be able to complain to the regulator. There is a similar provision in the Equal Opportunity Act.³⁷⁰ If the worker has already made a complaint about an act or practice, a complaint about victimisation will be able to be considered at the same time.



RECOMMENDATION(S)

53. The legislation should prohibit victimisation of workers (including prospective workers) by the employer.
54. An employer victimises a worker (including prospective workers) if the employer subjects or threatens to subject the worker to any detriment because the worker, or a person associated with the worker:
 - has made a complaint against the employer under the Act;
 - has given evidence or information, or produced a document, in connection with any proceedings under the Act;
 - has attended a conciliation conference;
 - has alleged that the employer has contravened the Act, unless the allegation is false and was not made in good faith;
 - has refused to do something that would contravene a provision of the Act;

369 Roundtable 3; submission 4.

370 *Equal Opportunity Act 1995* (Vic) ss 96, 97.

! RECOMMENDATION(S)

- because the worker has reasonable cause to believe the employer has done or intends to do any of the above.

ENSURING COMPLIANCE—SANCTIONS PYRAMID

4.75 The previous sections have discussed the regulator's powers to receive and resolve complaints, to investigate acts or practices which come to its attention while dealing with a complaint and to inquire into employer acts or practices which affect workers' privacy. This section deals with the sanctions which should apply in cases of non-compliance.

4.76 A number of regulatory theorists argue that compliance with a legislative regime is enhanced by a 'sanctions pyramid' approach.³⁷¹ This relies initially on encouraging conforming behaviour through information and education about legislative requirements. In the case of minor breaches, it will often be appropriate for the regulator to warn non-compliers and/or give them an informal opportunity to remedy the problem, before any penalty is imposed.

4.77 Serious or repeated breaches should result in the imposition of more severe penalties,³⁷² because 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.³⁷³ Commentators have noted that escalation of the regulatory response has the effect of channelling 'most of the regulatory action to the cooperative base of the pyramid',³⁷⁴ which allows employers to resolve issues in a cooperative manner³⁷⁵ and encourages corporate responsibility.³⁷⁶

4.78 Several consultation participants supported the concept of an escalating scale of sanctions,³⁷⁷ which allows the regulator to tailor the sanction³⁷⁸ both to the

371 Sanctions pyramid theory was discussed in VLRC (September 2004) n 16, para 4.14.

372 Submission 22.

373 Christine Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 (5) *Administration and Society* 529, 541. See also John Braithwaite, 'Responsive Business Regulatory Institutions' in CAJ Coady and CJG Sampford (eds) *Business Ethics and the Law* (1993) 84; Fiona Haines, *Corporate Regulation: Beyond Punish or Persuade* (1997) 219.

374 Braithwaite (1993), above n 373, 88.

375 Ibid 88–9.

376 Ibid 88.

377 Roundtables 4, 5.

seriousness of the identified breach and to the type of offender. Not surprisingly, unions tended to support the use of monetary penalties to ensure employer compliance, while employers and employer organisations were more likely to emphasise the importance of encouraging cooperation. One employer made the salient comment that it was not in anyone's interest to have regulation open to abuse by rogue organisations.³⁷⁹

4.79 The proposed workplace privacy scheme is consistent with this sanctions pyramid approach. The regulator's role in promoting workplace privacy is intended to encourage employers to comply voluntarily with the scheme. The regulator's power to resolve complaints informally, to conciliate complaints in appropriate cases and make rulings which can be enforced by registration at VCAT will assist in fostering respect for privacy.

4.80 It is only when these mechanisms fail that stronger sanctions should apply. In the next sections we discuss monetary penalties and compliance notices.

MONETARY PENALTIES

4.81 Breaches of information privacy principles under the Information Privacy Act and of health privacy principles under the Health Records Act are generally dealt with under complaints-resolution processes. The main exception to this principle is that it is a criminal offence to disobey a compliance notice served by the regulator, requiring compliance with the legislation.³⁸⁰

4.82 In general, we propose that breaches of workplace privacy requirements be dealt with in a similar way. Workers who are affected by a breach will be able to complain and have their complaint conciliated. In appropriate cases, the regulator will be able to make a ruling requiring the employer to resolve the problem. A similar approach will apply when the regulator identifies systemic breaches in the course of investigating a complaint.

4.83 However, we propose civil monetary penalties apply where:

- an employer breaches a prohibition in the legislation (eg the prohibition against surveillance in toilets etc);

378 Julia Black, 'Managing Discretion' (Paper presented at the ALRC Conference, Penalties: Policy, Principles and Practice in Government Regulation, Sydney, 7 June 2001) 25.

379 Roundtable 4.

380 *Information Privacy Act 2000* (Vic) s 48; *Health Records Act 2001* (Vic) s 71. Compliance notices are discussed in paras 4.89–4.91.

- an employer fails to report to the regulator about the action taken in respect of a ruling (there is an equivalent provision in the Health Records Act);³⁸¹
- an employer does not obtain an authorisation for an act or practice when required to do so under the legislation (authorisation is required for acts or practices affecting workers outside work, for genetic testing and other practices prescribed by regulation);
- an employer breaches an authorisation;
- an employer fails to obey a compliance notice (compliance notices are discussed below).

4.84 We propose that civil, and not criminal, penalties should apply to these breaches. This may be contrasted with the approach under the Surveillance Devices Act, which makes it a criminal offence to unlawfully use surveillance devices or unlawfully publish information obtained through use of these devices.³⁸²

4.85 Civil penalty amounts will vary according to the seriousness of the breach. The regulator can initiate proceedings to enforce the penalty in the Magistrates' Court.³⁸³

4.86 Some may argue that criminal penalties should be imposed to protect employees against unlawful surveillance. However, as we have pointed out, under the Surveillance Devices Act this offence will rarely apply in the context of workplace privacy because employers will usually obtain employee consent before using surveillance devices. Our proposals provide broader protection to workers against surveillance but impose civil penalties for breach in certain situations. In our view, this approach is more likely to encourage employers to adopt a cooperative approach to the proposed scheme rather than imposing criminal penalties.

4.87 The Australian Law Reform Commission defines a civil penalty as a punitive sanction which is often financial in nature and imposed outside the criminal process.³⁸⁴ The standard of proof for imposing a civil penalty is the balance of probabilities, rather than the criminal law standard which requires proof of an offence beyond reasonable doubt.

381 *Health Records Act 2001* (Vic) s 64(7).

382 See *Surveillance Devices Act 1999* (Vic) ss 6, 7, 8, 11, 12.

383 See clause 78 of the draft Bill.

384 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, Report No 95 (2002) 72–3.

4.88 The commission believes that the imposition of a civil penalty when other mechanisms fail to produce compliance will offer sufficient protection for workers. As is the case under other Victorian privacy laws, failure to appear before the regulator or obstructing the regulator will be criminal offences.³⁸⁵

! RECOMMENDATION(S)

55. The legislation should impose a civil penalty for:

- performing an act which is prohibited;
- failing to report to the regulator about action taken in response to a ruling;
- not seeking an authorisation for an act or practice which affects the privacy of workers while they are engaged in non-work-related activities;
- breaching an authorisation for an act or practice that affects the privacy of workers while they are engaged in non-work-related activities;
- not seeking an authorisation or breaching an authorisation for genetic testing.

OTHER STEPS TO ENSURE COMPLIANCE

4.89 Many workplace privacy issues will be resolved informally or through the conciliation process. Where this does not occur, we have recommended that the regulator have the power to make a ruling, which can be registered at VCAT and will have the effect of a VCAT order. It is likely that most employers will comply with rulings made by the regulator or VCAT.

385 *Information Privacy Act 2000* (Vic) s 65 (failure to attend before Privacy Commissioner or to obstruct the Privacy Commissioner), s 66 (communicating information relating to the affairs of an individual acquired in the exercise of powers under the Act), and see also s 48 (failure to comply with compliance notice); *Health Records Act 2000* (Vic) s 80 (unlawfully requiring consent), s 81 (unlawfully destroying or removing health information), s 83 (threatening or intimidating people to persuade them not to exercise rights under the Act), s 84 (failure to attend before the Health Services Commissioner), s 90 (communicating information relating to the affairs of an individual acquired in the exercise of powers under the Act) and see also s 71 (failure to comply with a compliance notice).

4.90 In some cases, the regulator may have reason to believe the employer is ignoring a ruling. Where this is the case, the regulator should have the power to initiate an investigation to determine whether the employer is complying with a ruling or a compliance notice (compliance notices are discussed in paragraph 4.91). We have recommended that when the regulator is investigating a complaint it should have the power to call witnesses, require production of documents, audit records, and monitor and report on the adequacy of equipment and user safeguards. These powers should also apply where the regulator is investigating compliance with a ruling or a notice.

COMPLIANCE NOTICES

4.91 Where the employer has committed a serious or flagrant breach of the legislation, we recommend the regulator have the power to issue a compliance notice which requires the employer to remedy the breach in question. A significant monetary penalty will be imposed if the employer fails to meet the requirements of a compliance notice and this penalty will be enforceable in the Magistrates' Court. The regulator's decision to issue a compliance notice will be reviewable by VCAT. The proposed compliance notice provisions mirror equivalent provisions contained in the Health Records Act,³⁸⁶ except that non-compliance will not be a criminal offence but will attract a civil penalty. The regulator will also have the power to investigate whether an employer is complying with a notice, which is discussed in more detail below.

POWER TO VIEW PREMISES AND EQUIPMENT

4.92 In most cases, the regulator's powers to request an employer to produce documents, require a person to attend and answer questions, audit records and monitor equipment will be sufficient to enable it to monitor compliance with the legislation.³⁸⁷ However, where the regulator has made a ruling or issued a compliance notice against an employer, we recommend that the regulator have the additional power to enter and inspect premises to ascertain whether the employer is satisfying its obligations.³⁸⁸

4.93 We do not anticipate that the regulator will frequently seek to enter premises. In most cases, information on compliance could be collected by exercising the powers

386 *Health Records Act 2001* (Vic) s 66.

387 Cf *Health Records Act 2001* (Vic) s 67.

388 This is not an unusual power for a regulator to be provided with—see, eg, the *Australian Securities and Investments Commission Act 2001* (Cth) ss 13, 35–7; *Trade Practices Act 1974* (Cth) s 155; *Occupational Health and Safety Act 2004* (Vic) pt 9, div 3.

mentioned above. In some limited cases, however, it may be necessary to view premises to see how equipment is set up or where it is located. For example, the regulator may wish to check on the location and signage associated with audio or video surveillance devices or to examine computer systems which monitor email or internet use. This power is set out in Part 6 of the draft Bill.

! RECOMMENDATION(S)

56. Where an employer fails to comply with a ruling made by the regulator or the employer has performed an act or used a practice which is a serious or flagrant contravention of the workplace privacy legislation, the regulator should have the power to serve a compliance notice on the employer.
57. The compliance notice may require the employer to refrain from an act or practice or to take specified action within a specified period of time and to report the taking of that action to the regulator.
58. A civil penalty should apply for failure to comply with a compliance notice.
59. The regulator should have the additional power to view premises and equipment where a ruling has been made or a compliance notice issued to ensure the employer is satisfying its obligations.

VCAT HEARING AND REVIEW

4.94 This section discusses the role of VCAT in overseeing the complaints-resolution process under the workplace privacy legislation. It deals with:

- VCAT's jurisdiction to hear a complaint;
- the orders which can be made by VCAT;
- VCAT's review jurisdiction;
- the role of the Supreme Court.

4.95 Both the Information Privacy Act and the Health Records Act provide for employers and workers to seek a VCAT hearing or to have a decision made by the regulator reviewed.³⁸⁹ Provision for a hearing or review by a separate body helps to ensure the legislation is perceived as fair and contributes to the accountability and legitimacy of the regulator's office.³⁹⁰ Such provisions can also improve the quality and consistency of the regulator's decisions and provide relatively inexpensive and efficacious remedies for workers and employers.

4.96 The Information Privacy Act and the Health Records Act provide for a matter to be referred to VCAT when:

- the commissioner declines to entertain a complaint and the complainant requires the commissioner to refer the matter to VCAT;³⁹¹
- the commissioner decides that conciliation is inappropriate and decides not to further entertain the complaint and the complainant requires the commissioner to refer the matter to VCAT;³⁹²
- conciliation fails and the complainant requires the commissioner to refer the matter to VCAT;³⁹³
- the commissioner investigates the complaint and makes a ruling on it and the dissatisfied complainant or respondent requires the regulator to refer the matter to VCAT.³⁹⁴

4.97 We propose that VCAT have similar jurisdiction to hear matters referred to it by the regulator under workplace privacy legislation, with one difference. As we explained in paragraphs 4.65–4.68, we propose that a ruling made by the regulator be enforceable if the respondent does not require the regulator to refer it to VCAT and the complainant registers the ruling.

389 *Information Privacy Act 2000* (Vic) pt 5, divs 4, 5; *Health Records Act 2001* (Vic) pt 6, divs 5, 6.

390 Black (2001), above n 378, 25; see ALRC (2003), above n 229, vol 2, 704.

391 See, eg, *Information Privacy Act 2001* (Vic) s 29(5); *Health Records Act 2001* (Vic) s 51(5).

392 See, eg, *Information Privacy Act 2001* (Vic) s 32(3); *Health Records Act 2001* (Vic) ss 56(4), 57.

393 See, eg, *Information Privacy Act 2001* (Vic) s 37(3); *Health Records Act 2001* (Vic) s 63(3).

394 See, eg, *Health Records Act 2001* (Vic) ss 64(3), 65. There is no similar process in the Information Privacy Act.

ORDERS MADE BY TRIBUNAL AFTER HEARING

4.98 After hearing the complaint, VCAT should have the power to make various orders to resolve it.³⁹⁵ Similar powers exist under the Information Privacy Act and the Health Records Act.³⁹⁶

TRIBUNAL REVIEW

4.99 The Information Privacy Act and the Health Records Act³⁹⁷ also give VCAT the jurisdiction to review, on its merits, a decision of the regulator to issue a compliance notice. We recommend that similar jurisdiction be conferred on VCAT to review a regulator's decision to issue a compliance notice under the workplace privacy legislation. On review, VCAT would have the power to uphold or reject the regulator's decision to issue a compliance notice. The regulator would be a party to an application for review.

INTERIM ORDERS

4.100 VCAT should also have the jurisdiction to make interim orders on the application of a complainant or respondent or the regulator to prevent a party to the complaint acting in a way which is prejudicial to negotiations or conciliation, or to any decision that the tribunal may subsequently make.³⁹⁸

SUPREME COURT APPEAL

4.101 We recommend that a party to VCAT proceedings be able to appeal to the Supreme Court on a question of law.



RECOMMENDATION(S)

60. VCAT should have jurisdiction to hear a complaint when:

395 These orders are set out in our recommendations. The power to order that the employer take action to redress the effects of the act or practice can include ordering an apology (see recommendation 61 on performing 'any reasonable act').

396 *Information Privacy Act 2000* (Vic) s 43; *Health Records Act 2001* (Vic) s 78.

397 *Health Records Act 2001* (Vic) ss 66, 71, 72; *Information Privacy Act 2000* (Vic) ss 44–49.

398 See, eg, *Information Privacy Act 2001* (Vic) s 38; *Health Records Act 2000* (Vic) s 73.

! RECOMMENDATION(S)

- the regulator declines to entertain a complaint and the complainant requires the regulator to refer the matter to VCAT for a hearing of the complaint;
 - the regulator decides that conciliation is inappropriate and decides not to further entertain the complaint and the complainant requires the regulator to refer the matter to VCAT;
 - conciliation fails and the complainant requires the regulator to refer the matter to VCAT;
 - the regulator makes a ruling and a complainant or respondent requires the regulator to refer the matter to VCAT.
61. Where, after a hearing, VCAT finds that a complaint is substantiated, it may make an order that:
- the employer must not repeat or continue the act or practice;
 - the employer must perform any reasonable act or undertake a course of conduct to redress any loss or damage suffered by the worker;
 - the worker is entitled to a specified amount not exceeding \$100,000 as compensation for any loss or damage suffered, including injury to the worker's feelings or humiliation suffered by the worker as a result of the employer's act or practice;
 - the employer publish, at the employer's expense, an advertisement as specified in the order;
 - any existing authorisation the employer possesses be revoked, or revoked until the employer performs another specified act.
62. Where the act or practice affects people other than the person making the complaint, VCAT may make a ruling to protect the privacy of people other than the person making the complaint if, having regard to the circumstances, it is appropriate to do so.
63. VCAT should have the jurisdiction to review a decision by the regulator to issue a compliance notice.

**RECOMMENDATION(S)**

64. VCAT should have the jurisdiction to make interim orders to prevent a party to a complaint from acting in a way which is prejudicial to conciliation or to any decision or order VCAT may subsequently make.
65. The Supreme Court's jurisdiction to hear appeals on questions of law from VCAT should apply to decisions under the workplace privacy legislation.

Appendix 1

ROUNDTABLES

| No | Date—2004 | Participants |
|----|------------|---|
| 1 | 6 October | Mr Paul Chadwick, Office of the Victorian Privacy Commissioner Dr Breen Creighton, Corrs Chambers Westgarth Lawyers Professor Peter Grabosky, Australian National University Dr Fiona Haines, University of Melbourne Mr David Lindsay, University of Melbourne Mr Chris Maxwell QC, barrister Ms Sue Walpole, Legal Practice Board Mr Nigel Waters, Australian Privacy Foundation |
| 2 | 11 October | Mr Joo-Cheong Tham, La Trobe University Mr Brian Corney, Industrial Relations Victoria Mr Brendon Gale, Australian Football League Players' Association Mr Leigh Hubbard, Victorian Trades Hall Council Mr Tim Lyons, National Union of Workers Mr Gavin Merriman and Ms Emma Walters, Australian Workers' Union Mr Raoul Wainwright and Mr Jesse Maddison, Construction, Forestry, Mining and Electrical Union Mr Richard Watts, Australian Council of Trade Unions |
| 3 | 18 October | Senior Sergeant Ken Burchett, Victoria Police Mr Jim Nolan, Barrister Professor Marilyn Pittard, Monash University Mr Paul Ryan, Victorian Transport Association Mr Peter Salway, Office of Public Employment Ms Leyla Yilmaz and Ms Liz Hayes, Victorian Automobile Chamber of Commerce |

| No | Date—2004 | Participants |
|----|------------|---|
| 4 | 20 October | Associate Professor Beth Gaze, Monash University Mr Andrew Dillon, Australian Football League Mr Darren Fewster and Ms Samantha Kennedy, Telstra Ms Kristina Flynn, Australian Industry Group Mr Ian Gilbert, Australian Bankers' Association Mr David Gregory, Victorian Employers' Chamber of Commerce Professor Ron McCallum, University of New South Wales Ms Suzanne Pigdon, Coles Myer |
| 5 | 28 October | Ms Gayle Hill, Freehills Ms Mary-Jane Ierodiconou, Blake Dawson Waldron Mr Stuart Kollmorgen, Deacons Mr David Lindsay, University of Melbourne Mr Charles Power, Holding Redlich Ms Melinda Richards, barrister Mr Peter Rozen, barrister |

Appendix 2

CONSULTATIONS

| No | Subject | Date—2003 | Participants |
|----|-----------------------------------|-------------|-------------------------------------|
| 1 | Email and internet monitoring | 20 October | technical experts |
| 2 | Psychological testing | 20 October | technical experts |
| 3 | Biometrics and surveillance | 22 October | technical experts |
| 4 | Testing and surveillance | 22 October | unions |
| 5 | Surveillance | 23 October | employer associations and employers |
| 6 | Surveillance | 23 October | unions |
| 7 | Email and internet monitoring | 24 October | employer associations and employers |
| 8 | Email and internet monitoring | 24 October | unions |
| 9 | Alcohol, drug and medical testing | 31 October | technical experts |
| 10 | Testing | 5 November | employer associations and employers |
| 11 | Testing | 5 November | unions |
| 12 | Surveillance | 11 November | unions |
| 13 | Testing | 12 November | employer associations |
| 14 | Email and internet monitoring | 14 November | employers |
| 15 | Email and internet monitoring | 18 November | unions |

| No | Subject | Date—2003 | Participants |
|----|--------------------------------------|-------------|-----------------------|
| 16 | Surveillance, monitoring and testing | 19 November | employers |
| 17 | Surveillance and testing | 20 November | employers |
| 18 | Surveillance | 20 November | employer associations |
| 19 | Testing | 21 November | unions |
| 20 | Testing | 21 November | employers |
| 21 | Testing and surveillance | 24 November | unions |

CONSULTATION PARTICIPANTS

EMPLOYER ASSOCIATIONS, EMPLOYERS AND UNIONS

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

Boulderstone 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 Boulton, 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, Monash University
Mr Mike Thompson, Linus

Appendix 3

OPTIONS PAPER SUBMISSIONS

| No | Name | Affiliation |
|----|-------------------------------------|--|
| 1 | Anonymous | |
| 2 | Simon Edwards | Microsoft Australia |
| 3 | David Eynon | Air Conditioning and Mechanical Contractors' Association of Victoria |
| 4 | Zana Bytheway | Job Watch Employment Rights Legal Centre |
| 5 | Dan Romanis | Royal District Nursing Service |
| 6 | Confidential | |
| 7 | Costa Brehas | Australian Hotels & Hospitality Association |
| 8 | Charles Heunemann | Surf Control |
| 9 | Joe De Bruyn | Shop, Distributive & Allied Employees Association |
| 10 | Arthur Crook | Australian Psychological Society |
| 11 | Ian Gilbert | Australian Bankers' Association |
| 12 | Rita Biviano | AXA Australian Pacific Holdings |
| 13 | Peter Jamwold | Insurance Council of Australia |
| 14 | Michael Wood | National Tertiary Education Union, Deakin University Branch |
| 15 | David Lynch | International Banks and Securities Association of Australia |
| 16 | Lisa Fitzpatrick | Australian Nursing Federation |
| 17 | Beth Wilson c/o Michael McDonald | Office of the Health Services Commissioner |

| No | Name | Affiliation |
|----|--------------------------------------|---|
| 18 | Tony Keenan | Victorian Independent Education Union |
| 19 | Peter Croft | Clearswift Asia Pacific |
| 20 | Prof Lyndsay Neilson | Department of Sustainability and Environment |
| 21 | David Lynch (repeated) | International Banks and Securities Association of Australia |
| 22 | Leyla Yilmaz | Victorian Automobile Chamber of Commerce |
| 23 | Allan Mulvena | Electrical Trades Union (Southern States Branch) |
| 24 | Allens Arthur Robinson | |
| 25 | Brian Donegan | Australian Retailers Association Victoria |
| 26 | Dr Helen Szoke | Equal Opportunity Commission Victoria |
| 27 | Suzanne Pigdon and Paul Duckett | Coles Myer Limited |
| 28 | Leigh Hubbard | Victorian Trades Hall Council |
| 29 | Sandra Parker | Department of Employment and Workplace Relations |
| 30 | John Ryan | Association of Needle and Syringe Programs |
| 31 | Dave Oliver | Australian Manufacturing Workers' Union |
| 32 | Acting Inspector Anthony O'Connor | Victoria Police |
| 33 | Victoria Strong | Law Institute of Victoria |
| 34 | Sarah Roberts | National Tertiary Education Union |
| 35 | Anonymous | |
| 36 | Samantha Kennedy | Telstra Corporation Limited |

Appendix 4

ISSUES PAPER SUBMISSIONS

| No | Name | Affiliation |
|----|------------------|---|
| 1 | Brian Boyd | Victorian Trades Hall Council |
| 2 | Dr 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 |
| 12 | Kate Rattigan | Conduct and Ethics Unit, Department of Education and Training |
| 13 | Murray Smith | Leader Community Newspapers |
| 14 | Dave Oliver | Australian Manufacturing Workers' Union |
| 15 | Lindy Smith | Australian Privacy Foundation |
| 16 | Paul Begley | Australian Human Resources Institute |
| 17 | Dr Trevor Kerr | Southern Health Pathology |
| 18 | Gwynn Boyd | Minorplanet Asia Pacific Pty Ltd |
| 19 | Confidential | |
| 20 | John McGinness | Commonwealth Attorney-General's Department |
| 21 | Peter Sanader | The Tout, On Track and Ratings |
| 22 | Dr Diane Sisely | Equal Opportunity Commission Victoria |

| No | Name | Affiliation |
|----|--|--|
| 23 | Mervyn K Vogt | |
| 24 | Dan Romanis | Royal District Nursing Service |
| 25 | John T Rush | Victorian Bar |
| 26 | Ian Gilbert | Australian Bankers' Association |
| 27 | Dr Margaret Otlowski | Faculty of Law—University of Tasmania |
| 28 | Elizabeth Hayes | Victorian Automobile Chamber of Commerce |
| 29 | Helen Versey | Office of the Victorian Privacy Commissioner |
| 30 | Julie Phillips | |
| 31 | Chief Commissioner Christine Nixon APM | Victoria Police |
| 32 | Anonymous | |
| 33 | Eileen Tubb | |
| 34 | Alan Dudderidge | Transport Watchhousing Industry |

Appendix 5

DRAFT BILL—OFFICE OF THE CHIEF PARLIAMENTARY COUNSEL

Workplace Privacy Act 2005

Act No.

TABLE OF PROVISIONS

Clause

PART 1—PRELIMINARY

1. Purposes
2. Commencement
3. Definitions
4. When use of surveillance device may constitute covert surveillance
5. Employer must inform and consult with workers
6. Nature of rights created by this Act
7. Crown to be bound

PART 2—EMPLOYERS' DUTIES

Division 1—Protection of Privacy (Work-Related Activities)

8. Protection of privacy of workers—work-related activities

Division 2—Acts or Practices Requiring Authorisation

9. Protection of privacy of workers—non-work-related activities
10. Protection of privacy of workers—genetic testing
11. Application for review—authorisation

Division 3—Surveillance Device Prohibition

12. Prohibition on certain uses of surveillance devices

PART 3—CODES OF PRACTICE

Division 1—Advisory Codes of Practice

13. Advisory codes of practice
14. Procedure for code or variation
15. Commencement of advisory code or variation
16. Effect of advisory code of practice
17. Revocation of advisory code of practice
18. Disallowance of regulator's decision

Division 2—Approved Codes of Practice

19. Approved codes of practice
20. Procedure for obtaining approval of code or variation
21. Commencement of approved code or variation
22. Employers bound by approved code of practice
23. Effect of approved code of practice
24. Approved codes of practice register
25. Revocation of approval
26. Disallowance of regulator's decision

Division 3—Mandatory Codes of Practice

27. Mandatory codes of practice
28. Procedure for obtaining approval of mandatory code, variation or revocation
29. Commencement of mandatory code, variation or revocation
30. Effect of mandatory code of practice
31. Effect of revocation of mandatory code of practice

PART 4—COMPLAINTS

Division 1—Making a Complaint

32. Who may complain?
33. Complaint

Division 2—Procedure after a Complaint is Made

34. Regulator must notify respondent
35. Preliminary assessment of complaint
36. Splitting complaints
37. Circumstances in which regulator may decline to entertain complaint
38. Regulator may dismiss stale complaint
39. Acceptance of complaint
40. What happens if conciliation or ruling is inappropriate?
41. Duty to stop proceedings

Division 3—Conciliation of Complaints

42. Conciliation process
43. Power to obtain information and documents
44. Conciliation agreements
45. Conciliation statements, acts and documents inadmissible
46. What happens if conciliation fails?

Division 4—Investigations, Rulings and Compliance Notices

47. Investigation and ruling
48. Referral to Tribunal
49. Enforcement of ruling
50. Compliance notice
51. Power to obtain information and documents
52. Power to examine witnesses
53. Conduct of investigation etc.
54. Protection against self-incrimination
55. Failure to comply with compliance notice
56. Application for review—compliance notice

Division 5—Interim Orders

57. Tribunal may make interim orders before hearing

Division 6—Jurisdiction of the Tribunal

58. When may the Tribunal hear a complaint?
59. Who are the parties to a proceeding?
60. What may the Tribunal decide?

PART 5—OTHER INVESTIGATIONS AND INQUIRIES**Division 1—Investigations Initiated by the Regulator**

61. When can the regulator initiate an investigation?
62. Conduct of investigation
63. Powers in conducting an investigation
64. Protection against self-incrimination
65. Referral to Tribunal
66. Order by the Tribunal

Division 2—Inquiries Undertaken by the Regulator

67. When can the regulator initiate an inquiry?
68. Conduct of inquiry
69. Power to obtain information and documents and power to examine witnesses
70. Regulator to give opportunity for making submissions
71. Report to contain recommendations

72. Reports to be tabled in Parliament

PART 6—POWER TO VIEW PREMISES AND SYSTEMS

73. Searches to monitor compliance with Act
74. Operation of electronic equipment at premises
75. Power to require information or documents
76. Protection against self-incrimination

PART 7—ENFORCEMENT

Division 1—Civil Penalties

77. Conduct attracting civil penalties
78. Proceedings for contravention of civil penalty provision
79. Conduct in contravention of more than one civil penalty provision
80. Application and enforcement of civil penalties

Division 2—Criminal penalties

81. Failure to attend etc. before regulator
82. Secrecy
83. Offences by bodies
84. Prosecutions

Division 3—Employees and Agents

85. Employees and agents

PART 8—GENERAL

Division 1—The Regulator

86. Appointment of the regulator
87. Remuneration and allowances
88. Terms and conditions of appointment
89. Vacancy, resignation
90. Suspension of the regulator
91. Acting appointment
92. Validity of acts and decisions
93. Staff
94. Functions of the regulator
95. Powers of the regulator
96. Immunity of regulator
97. Delegation
98. Annual report
99. Other reports

Division 2—Victimisation

100. Victimisation of worker

Division 3—Regulations

101. Regulations

Division 4—Amendment of Acts

102. Amendment of Victorian Civil and Administrative Tribunal Act 1998
 103. Amendment of Public Administration Act 2004
-
-

A BILL

to regulate the practices of surveillance, monitoring, tracking, searching and testing of workers, to amend the **Victorian Civil and Administrative Tribunal Act 1998** and the **Public Administration Act 2004** and for other purposes.

Workplace Privacy Act 2005

The Parliament of Victoria enacts as follows:

PART 1—PRELIMINARY

1. Purposes

The purposes of this Act are—

- (a) to provide privacy protection for workers without unduly limiting the legitimate interests of employers in the conduct of their business; and

Workplace Privacy Act 2005

Act No.

Part 1—Preliminary

- (b) to assist in giving effect to Australia's international obligations in relation to the human right of privacy recognised in Article 17 of the International Covenant on Civil and Political Rights.

2. Commencement

- (1) This Act, except Parts 4 and 5, comes into operation on the day after the day on which it receives the Royal Assent.
- (2) Subject to sub-section (3), Parts 4 and 5 come into operation on a day or days to be proclaimed.
- (3) If a provision of Part 4 or 5 does not come into operation before [*specified date*], it comes into operation on that day.

3. Definitions

- (1) In this Act—

"act or practice", in relation to a worker or a prospective worker, includes—

- (a) the use of a surveillance device; and
- (b) the use of any other device to observe, listen to, record, track, monitor or search a worker or prospective worker; and
- (c) the taking of a sample of breath, blood, saliva or urine or of any other bodily substance for the purpose of testing for the presence of alcohol or drugs; and
- (d) the use of a psychometric test or a medical test; and
- (e) the use of a genetic test; and
- (f) the use of a biometric measure; and
- (g) the use of any other means to search a worker or prospective worker;

"advisory code of practice" means a code of practice issued under section 13(1) as varied and in operation for the time being;

"approved code of practice" means a code of practice approved under section 20 as varied and in operation for the time being;

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

- "biometric measure"** means any device or technique used to identify a person on the basis of physical or behavioural characteristics;
- "business"** includes activities carried on for a charitable or other non-profit purpose;
- "business day"** means a day other than a Saturday, a Sunday or a public holiday appointed under the **Public Holidays Act 1993**;
- "child"** means a person under the age of 18 years;
- "civil penalty provision"** means a provision referred to in section 77(1);
- "communication"** includes all information, in whatever form, that forms part of, or is attached to or associated with, a communication;
- "communications system"** means a system for generating, sending, receiving, storing or otherwise processing communications and includes all infrastructure components that are comprised in the system and all devices utilised by or in the system;
- "consent"** means express consent;
- "device"** includes instrument, apparatus, equipment and computer program;
- "disability"**, in relation to a person, means intellectual impairment, mental disorder, brain injury, physical disability or dementia;
- "document"** includes any computer program by means of which any data or image embodied in the document may be reproduced;
- "employer"** means a person, body or firm that—
- (a) employs another person under a contract of service or apprenticeship; or
 - (b) employs another person under the **Public Administration Act 2004** or any other Act; or
 - (c) engages another person under a contract for services; or

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

- (d) engages another person to perform any work the remuneration for which is based wholly or partly on commission; or
- (e) engages a volunteer to perform work; or
- (f) in the case of a worker who is a bailee of a taxi-cab, a restricted hire vehicle or a special purpose vehicle, the bailor of the vehicle;

"firm" has the same meaning as in the **Partnership Act 1958**;

"genetic testing" means the use of samples obtained from the body of a worker or prospective worker for the purpose of obtaining information about an existing or future health condition of, or the characteristics of, the worker or prospective worker;

"mandatory code of practice" means a code of practice approved under section 28 as varied and in operation for the time being;

"optical surveillance device" has the same meaning as in the **Surveillance Devices Act 1999**;

"premises" means premises owned or controlled by an employer;

"privacy" means the human right of privacy recognised in Article 17 of the International Covenant on Civil and Political Rights;

"property" means all real and personal property, including money, choses in action, trade secrets, intellectual property and other intangible property;

"proportionate", in relation to an act or practice, means the act or practice that achieves the purpose for which it is undertaken but interferes least with the privacy of the worker or workers concerned;

"prospective worker" means an applicant for a position as a worker;

"restricted hire vehicle" has the same meaning as in section 86 of the **Transport Act 1983**;

"special purpose vehicle" has the same meaning as in section 86 of the **Transport Act 1983**;

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

- "surveillance device"** includes a surveillance device within the meaning of the **Surveillance Devices Act 1999** and any other device for monitoring or observing electronic or other communications;
- "taxi-cab"** has the same meaning as in section 86 of the **Transport Act 1983**;
- "the regulator"** means the Privacy Commissioner appointed under Part 7 of the **Information Privacy Act 2000** or any other person appointed by the Minister under section 86(1) as the regulator;
- "the Tribunal"** means the Victorian Civil and Administrative Tribunal established by the **Victorian Civil and Administrative Tribunal Act 1998**;
- "tracking device"** has the same meaning as in the **Surveillance Devices Act 1999**;
- "volunteer"** means a person engaged by an employer to perform work on an unpaid or voluntary basis but does not include a person who is engaged by another person on an unpaid or voluntary basis to perform services in connection with that person's family or domestic affairs;
- "worker"** means—
- (a) a person employed under a contract of service or apprenticeship; or
 - (b) a person employed under the **Public Administration Act 2004** or any other Act or appointed to a statutory office; or
 - (c) a person engaged under a contract for services; or
 - (d) a person engaged to perform any work the remuneration for which is based wholly or partly on commission; or
 - (e) a volunteer; or
 - (f) a bailee of a taxi-cab, a restricted hire vehicle or a special purpose vehicle;
- "workplace"** means any place where workers perform work;

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

"work-related activity" includes—

- (a) an activity engaged in by a worker in the course of performing work for an employer at the premises of the employer or at any other place (except the worker's home or residence); and
 - (b) any use of the communications system of the employer, wherever the worker is located; and
 - (c) in the case of a bailee of a taxi-cab, a restricted hire vehicle or a special purpose vehicle, an activity engaged in under the contract of bailment.
- (2) In Part 4 and Part 8, Division 2, a reference to "worker" includes a reference to "prospective worker".

4. When use of surveillance device may constitute covert surveillance

For the purposes of this Act, the use by an employer in the workplace of a surveillance device is covert surveillance unless—

- (a) in the case of any surveillance device, each worker of the employer in the workplace has been notified by the employer in writing of the intended surveillance at least 14 days before the use of the device or, in the case of a worker who is first engaged as such a worker within that period of 14 days or at any time following its expiration, before commencing work; and
- (b) in the case of an optical surveillance device—
 - (i) the device or its casing, or other equipment that would generally indicate the presence of an optical surveillance device, is clearly visible in that part of the workplace in which the device is being used; and
 - (ii) a sign giving notice of the use of an optical surveillance device is clearly visible in any part of the workplace in which a device is being used; and
- (c) in the case of a tracking device, a sign giving notice of the use of the device is clearly visible to the worker or workers affected.

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

5. Employer must inform and consult with workers

If this Act refers to an employer informing and consulting with workers of the employer in relation to an act or practice, the employer—

- (a) when considering whether or not to introduce the act or practice, must inform those workers of—
 - (i) the act or practice being considered and the reason for its proposed introduction; and
 - (ii) the number, and categories, of workers likely to be affected by the act or practice; and
 - (iii) the anticipated date of introduction of the act or practice; and
 - (iv) the anticipated period during which the act or practice is proposed to be implemented; and
 - (v) any alternative acts or practices considered and the reasons why they were not considered appropriate; and
 - (vi) the safeguards to be used to ensure that the act or practice is conducted appropriately, having regard to the obligations in this Part; and
- (b) must provide those workers with a genuine opportunity to respond to the proposal; and
- (c) must take those responses into account when deciding whether or not to introduce the act or practice.

6. Nature of rights created by this Act

- (1) Nothing in this Act—
 - (a) gives rise to any civil cause of action; or
 - (b) without limiting paragraph (a), operates to create in any person any legal right enforceable in a court or tribunal—

other than in accordance with the procedures set out in this Act.
- (2) A contravention of this Act does not create any criminal liability except to the extent expressly provided by this Act.

*Workplace Privacy Act 2005**Act No.*

Part 1—Preliminary

7. Crown to be bound

This Act binds the Crown in right of Victoria and, so far as the legislative power of the Parliament permits, the Crown in all its other capacities.

*Workplace Privacy Act 2005**Act No.*

Part 2—Employers' Duties

PART 2—EMPLOYERS' DUTIES**Division 1—Protection of Privacy (Work-Related Activities)****8. Protection of privacy of workers—work-related activities**

- (1) An employer must not engage in an act or practice that unreasonably breaches the privacy of a worker or prospective worker when the worker or prospective worker is engaged in a work-related activity.
- (2) For the purposes of this section, an employer unreasonably breaches the privacy of a worker or prospective worker if the employer engages in an act or practice, in relation to work-related activities—
 - (a) for a purpose that is not directly connected to the business of the employer; or
 - (b) in a manner that is not proportionate to the purpose of the act or practice; or
 - (c) without first taking reasonable steps to inform and consult with workers of the employer concerning the act or practice, in accordance with section 5; or
 - (d) without providing adequate safeguards to ensure that the act or practice is conducted appropriately, having regard to the obligation in sub-section (1).
- (3) It is irrelevant whether an employer contravenes this section acting alone or in association with any other person.

Note: The regulator can issue advisory codes of practice to provide guidance to employers on how to comply with this section (see Part 3, Division 1). An employer may also comply with this section by complying with a binding approved code of practice (see Part 3, Division 2). An employer must comply with a mandatory code of practice in order to comply with this section (see Part 3, Division 3).

Division 2—Acts or Practices Requiring Authorisation**9. Protection of privacy of workers—non-work-related activities**

- (1) An employer must not, without authorisation by the regulator under sub-section (2) or by the Tribunal under section 11—

*Workplace Privacy Act 2005**Act No.*

Part 2—Employers' Duties

- (a) engage in an act or practice that breaches the privacy of a worker when the worker is engaged in an activity that is not a work-related activity; or
 - (b) engage in any other act or practice that is prescribed for the purposes of this section.
- (2) The regulator may, on application in writing by an employer, authorise the employer to engage in an act or practice referred to in sub-section (1) if the regulator is satisfied that—
- (a) there are reasonable grounds for believing that the worker's non-work-related activity may have a direct and serious impact on the business or reputation of the employer; and
 - (b) the act or practice cannot reasonably be undertaken while the worker is engaged in work-related activities; and
 - (c) the act or practice is proportionate to the protection of the employer's interests; and
 - (d) the employer will inform and consult workers concerning the act or practice in accordance with section 5 and ensure that the act or practice is conducted appropriately; and
 - (e) the employer has provided adequate safeguards to minimise interference with the worker's privacy.
- (3) An employer must comply with the terms of any authorisation.

10. Protection of privacy of workers—genetic testing

- (1) An employer must not, without authorisation by the regulator under sub-section (2) or by the Tribunal under section 11, conduct genetic testing of workers or prospective workers.
- (2) The regulator may, on application by an employer, authorise an employer to conduct genetic testing of workers or prospective workers if the regulator is satisfied that—
 - (a) the workers have consented to being genetically tested;
 - (b) there is substantial evidence of a connection between the working environment and the existence of, or a pre-disposition to, a condition that—

*Workplace Privacy Act 2005**Act No.*

Part 2—Employers' Duties

- (i) is detectable by genetic testing; and
 - (ii) has the potential to seriously endanger the health and safety of workers or others in the workplace;
 - (c) there are no other reasonable means of reducing or eliminating the workplace hazard;
 - (d) there are no other reasonable means of detecting the condition referred to in paragraph (b);
 - (e) the proposed genetic test sought to be authorised is scientifically reliable;
 - (f) the employer will use adequate safeguards to ensure that the test is conducted appropriately;
 - (g) the employer has informed and consulted with workers about the testing in accordance with section 5.
- (3) An employer must comply with the terms of any authorisation.

11. Application for review—authorisation

- (1) A worker or employer whose interests are affected by a decision of the regulator under section 9 or 10 to authorise or refuse to authorise an act or practice may apply to the Tribunal for review of the decision.
- (2) An application for review must be made within 28 days after the later of—
 - (a) the day on which the decision is made; or
 - (b) if, under the **Victorian Civil and Administrative Tribunal Act 1998**, the person requests a statement of reasons for the decision, the day on which the statement of reasons is given to the person or the person is informed under section 46(5) of that Act that a statement of reasons will not be given.
- (3) The regulator is a party to a proceeding on a review under this section.

*Workplace Privacy Act 2005**Act No.*

Part 2—Employers' Duties

Division 3—Surveillance Device Prohibition**12. Prohibition on certain uses of surveillance devices**

Without limiting section 8, an employer must not use a surveillance device to observe, listen to, record or monitor the activities, conversations or movements of a worker—

- (a) in a toilet, change room, lactation room or wash room in the workplace; or
 - (b) in any other prescribed circumstances.
-

Workplace Privacy Act 2005

Act No.

Part 3—Codes of Practice

PART 3—CODES OF PRACTICE

Division 1—Advisory Codes of Practice

13. Advisory codes of practice

- (1) For the purpose of providing guidance to employers concerning their duties or obligations under this Act, the regulator may, by notice published in the Government Gazette—
 - (a) issue advisory codes of practice in relation to any act or practice other than an act or practice referred to in section 9, 10 or 12; or
 - (b) vary any advisory code of practice issued by the regulator under paragraph (a).
- (2) An advisory code of practice must be consistent with section 8.
- (3) An advisory code of practice may apply, adopt or incorporate any matter contained in any document, whether wholly or partially or as amended by the code of practice.
- (4) An advisory code of practice—
 - (a) may be of general or limited application;
 - (b) may differ according to differences in time, place or circumstances.

14. Procedure for code or variation

- (1) Before exercising a power conferred by section 13(1), the regulator must cause a notice of intention to issue or vary an advisory code of practice to be published—
 - (a) in the Government Gazette; and
 - (b) in a daily newspaper circulating generally in Victoria.
- (2) A notice under sub-section (1) must—
 - (a) state where copies of the advisory code of practice (as proposed to be issued or varied) may be obtained; and
 - (b) specify a period of not less than 28 days after the date of the notice for making submissions on it to the regulator.

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (3) After considering any submissions received, the regulator may proceed under section 13(1), as proposed or with any amendments that the regulator considers appropriate.

15. Commencement of advisory code or variation

An advisory code of practice or variation comes into operation at the beginning of—

- (a) the day on which the notice under section 13(1) is published in the Government Gazette; or
- (b) any later day that is expressed in that notice as the day on which the code or variation comes into operation.

16. Effect of advisory code of practice

If an advisory code of practice is in operation in relation to an act or practice—

- (a) an employer who complies with the advisory code of practice in relation to the act or practice is, for the purposes of this Act, taken to have complied with section 8 in relation to that act or practice; and
- (b) an act or practice engaged in by an employer that contravenes the advisory code of practice is, for the purposes of this Act, taken to be a contravention of this Act unless the employer complies with section 8 in another way.

17. Revocation of advisory code of practice

- (1) The regulator may, by notice published in the Government Gazette, revoke an advisory code of practice.
- (2) The revocation comes into operation at the beginning of—
 - (a) the day on which the notice under sub-section (1) is published in the Government Gazette; or
 - (b) any later day that is expressed in that notice as the day on which the revocation comes into operation.

18. Disallowance of regulator's decision

The Governor in Council may at any time, by notice published in the Government Gazette, disallow a decision of the regulator to issue or

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

vary an advisory code of practice or to revoke an advisory code of practice.

Division 2—Approved Codes of Practice**19. Approved codes of practice**

- (1) An employer can comply with section 8 by complying with a code of practice approved under section 20 and binding on the employer.
- (2) An approved code of practice must be consistent with section 8.
- (3) An approved code of practice must not relate to an act or practice or class of act or practice to which a mandatory code of practice applies.
- (4) An approved code of practice may apply, adopt or incorporate any matter contained in any document, whether wholly or partially or as amended by the code of practice.
- (5) An approved code of practice—
 - (a) may be of general or limited application;
 - (b) may differ according to differences in time, place or circumstances.

20. Procedure for obtaining approval of code or variation

- (1) An employer may seek approval of a code of practice, or of a variation of an approved code of practice, by submitting the code or variation to the regulator.
- (2) The regulator may approve a code of practice, or a variation of an approved code of practice, submitted under sub-section (1).
- (3) Before exercising a power conferred by sub-section (2), the regulator must cause a notice of intention to issue or vary an approved code of practice to be published—
 - (a) in the Government Gazette; and
 - (b) in a daily newspaper circulating generally in Victoria.
- (4) A notice under sub-section (3) must—
 - (a) state where copies of the approved code of practice (as proposed to be issued or varied) may be obtained; and

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (b) specify a period of not less than 28 days after the date of the notice for making submissions on it to the regulator.
- (5) After considering any submissions received, the regulator may proceed under sub-section (2), as proposed or with any amendments that the regulator considers appropriate.

21. Commencement of approved code or variation

An approved code of practice or variation comes into operation at the beginning of—

- (a) the day on which the notice under section 20(3) is published in the Government Gazette; or
- (b) any later day that is expressed in that notice as the day on which the code or variation comes into operation.

22. Employers bound by approved code of practice

- (1) An approved code of practice binds—
 - (a) any employer that sought approval of it; and
 - (b) any employer that, by notice in writing given to the regulator, states that it intends to be bound by the approved code of practice as it is then in operation and that is capable of applying to the employer.
- (2) A notice under sub-section (1)(b) may indicate an intention that the employer be bound by the approved code of practice—
 - (a) generally; or
 - (b) only in respect of any specified act or practice or class of act or practice.
- (3) A notice under sub-section (1)(b) has no effect unless the regulator approves it.
- (4) The regulator may approve a notice under sub-section (1)(b) if satisfied that the approved code of practice is capable of applying to the employer to the extent set out in the notice.
- (5) An employer is bound by an approved code of practice—

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (a) in the case of an employer referred to in sub-section (1)(a), on and from the coming into operation of the code; and
 - (b) in the case of an employer referred to in sub-section (1)(b), on and from the date expressed in the notice under that sub-section as the date on and from which the employer will be bound by the code or the date on which the employer is notified of the regulator's approval of the notice, whichever is the later.
- (6) An employer bound by an approved code of practice may, by notice in writing given to the regulator, state that it intends to cease to be bound by that code.
- (7) An employer ceases to be bound by an approved code of practice on and from the date of the notice under sub-section (6) or such later date as is expressed in that notice as the date on and from which the employer will cease to be bound by the code.

23. Effect of approved code of practice

If an approved code of practice is in operation and binding on an employer, an act or practice engaged in by the employer that contravenes the code is, for the purposes of this Act, deemed to be a contravention of section 8.

24. Approved codes of practice register

- (1) The regulator must cause a register of all approved codes of practice to be established and maintained and for that purpose may determine the form of the register.
- (2) A person may during business hours—
 - (a) inspect the register and any documents that form part of it; or
 - (b) on the payment of any fee required by the regulations, obtain a copy of any entry in, or document forming part of, the register.

25. Revocation of approval

- (1) The regulator may, by notice published in the Government Gazette, revoke the approval of a code of practice or the approval of a variation of an approved code of practice.

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (2) The regulator may act under sub-section (1) on his or her own initiative or on an application for revocation made to him or her by an individual or employer.
- (3) Before deciding whether or not to revoke the approval of a code of practice or the approval of a variation of an approved code of practice, the regulator—
 - (a) must consult the employer that sought approval of the code or variation and may consult any other person or body that the regulator considers it appropriate to consult; and
 - (b) must have regard to the extent to which members of the public have been given an opportunity to comment on the proposed revocation.
- (4) An approved code of practice or approved variation ceases to be in operation at the beginning of—
 - (a) the day on which the notice of revocation under sub-section (1) is published in the Government Gazette; or
 - (b) such later day as is expressed in that notice as the day on which the code or variation ceases to be in operation.

26. Disallowance of regulator's decision

The Governor in Council may at any time, by notice published in the Government Gazette, disallow a decision of the regulator to issue or vary an approved code of practice or to revoke an approved code of practice.

Division 3—Mandatory Codes of Practice**27. Mandatory codes of practice**

- (1) As soon as reasonably practicable after the commencement of this section the regulator must prepare and seek approval under section 28 of a mandatory code of practice in relation to each of the following acts or practices—
 - (a) covert surveillance of workers in the workplace;

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (b) the taking from workers and prospective workers of samples of breath, blood, saliva or urine or of any other bodily substance for the purpose of testing for the presence of alcohol or drugs;
 - (c) any other act or practice that is prescribed for the purposes of this section.
- (2) A mandatory code of practice must be consistent with section 8.
 - (3) A mandatory code of practice may apply, adopt or incorporate any matter contained in any document, whether wholly or partially or as amended by the code of practice.
 - (4) A mandatory code of practice—
 - (a) may be of general or limited application;
 - (b) may differ according to differences in time, place or circumstances.

28. Procedure for obtaining approval of mandatory code, variation or revocation

- (1) The regulator may seek approval of a mandatory code of practice, or of a variation or revocation of a mandatory code of practice, in accordance with this section.
- (2) The Governor in Council, on the recommendation of the Minister acting on the advice received from the regulator under sub-section (3), may, by notice published in the Government Gazette, approve a mandatory code of practice or a variation or revocation of a mandatory code of practice.
- (3) The regulator may advise the Minister to recommend to the Governor in Council that a mandatory code of practice, or a variation or revocation of a mandatory code of practice, be approved.
- (4) The regulator may only advise that a mandatory code of practice, or a variation of a mandatory code of practice, be approved if, in the opinion of the regulator, the code or variation is consistent with this Act in relation to the act or practice to which the code applies.
- (5) Before deciding whether or not to advise the Minister to recommend approval of a mandatory code of practice, or approval of a variation or revocation of a mandatory code of practice, the regulator—

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

- (a) may consult any person or body that the regulator considers it appropriate to consult; and
 - (b) must cause a notice of intention to recommend approval of a mandatory code of practice or approval of a variation or revocation of a mandatory code of practice to be published—
 - (i) in the Government Gazette; and
 - (ii) in a daily newspaper circulating generally in Victoria.
- (6) A notice under sub-section (5)(b) must—
- (a) state where copies of the mandatory code of practice (as proposed to be issued, varied or revoked) may be obtained; and
 - (b) specify a period of not less than 28 days after the date of the notice for making submissions on it to the regulator.
- (7) After carrying out any consultations in accordance with sub-section (5)(a) and considering any submissions received in response to the notice under sub-section (6)(b), the regulator may proceed to advise the Minister as referred to in sub-section (3).

29. Commencement of mandatory code, variation or revocation

A mandatory code of practice, or a variation or revocation of a mandatory code of practice, comes into operation at the beginning of—

- (a) the day on which the notice of approval under section 28(2) is published in the Government Gazette; or
- (b) any later day that is expressed in that notice as the day on which the code, variation or revocation comes into operation.

30. Effect of mandatory code of practice

- (1) An employer must comply with a mandatory code of practice.
- (2) If a mandatory code of practice is in operation and binding on an employer, an act or practice engaged in by the employer that contravenes the code is, for the purposes of this Act, deemed to be a contravention of section 8.

*Workplace Privacy Act 2005**Act No.*

Part 3—Codes of Practice

31. Effect of revocation of mandatory code of practice

If a mandatory code of practice in relation to an act or practice is revoked, the regulator must seek approval under section 28 of another mandatory code of practice in relation to that act or practice.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

PART 4—COMPLAINTS**Division 1—Making a Complaint****32. Who may complain?**

- (1) The following may complain to the regulator—
 - (a) a worker who claims that an act or practice may be a breach of the privacy of the worker;
 - (b) if the worker is unable to complain because of disability—
 - (i) a person authorised by the worker to act on his or her behalf; or
 - (ii) if the worker is unable to authorise another person, any person who, by law, is entitled to act on his or her behalf;
 - (c) if the worker is a child—
 - (i) the child; or
 - (ii) a parent of the child on the child's behalf; or
 - (iii) if the regulator is satisfied that the child or a parent of the child so consents, any other person on the child's behalf.
- (2) An authorisation under sub-section (1)(b)(i) may be given—
 - (a) in writing; or
 - (b) in any other manner approved by the regulator.
- (3) In the case of an act or practice that may be a breach of the privacy of 2 or more workers, any one of those workers may make a complaint under sub-section (1) on behalf of all of the workers with their consent.
- (4) A representative body may make a complaint under sub-section (1) on behalf of a worker or workers if the representative body has a sufficient interest in the complaint.
- (5) A representative body has sufficient interest in a complaint if the act or practice that is the subject of the complaint is a matter of genuine concern to the body because of the way an act or practice of that kind

Workplace Privacy Act 2005
Act No.
Part 4—Complaints

adversely affects, or has the potential adversely to affect, the interests of the body or the interests or welfare of the workers it represents.

33. Complaint

- (1) A complaint must be in writing signed by, or on behalf of, the worker and lodged with the regulator.
- (2) A complaint must set out details of the alleged breach of privacy of the worker.
- (3) The regulator must provide appropriate assistance to a worker who wishes to make a complaint and requires assistance in formulating it.
- (4) A complaint must specify the respondent to it.
- (5) If the employer represents the Crown, the State is the respondent.
- (6) If the employer does not represent the Crown and—
 - (a) is a legal person, the employer is the respondent; or
 - (b) is an unincorporated body, the members of the committee of management of the employer are the respondents.
- (7) A failure to comply with sub-section (4) does not render the complaint, or any step taken in relation to it, a nullity.

Division 2—Procedure after a Complaint is Made

34. Regulator must notify respondent

The regulator must notify the respondent in writing of the complaint as soon as practicable after receiving it.

35. Preliminary assessment of complaint

- (1) As soon as reasonably practicable, and no later than 60 days, after the day on which a complaint is lodged, the regulator must decide whether, and to what extent, to entertain the complaint.
- (2) To enable the regulator to make a decision under sub-section (1), he or she may, by written notice, invite any person—
 - (a) to attend before the regulator for the purpose of discussing the subject-matter of the complaint; or
 - (b) to produce any documents specified in the notice.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (3) If the regulator considers it appropriate, he or she may attempt to resolve the complaint informally.

36. Splitting complaints

- (1) If a complaint—
- (a) deals with more than one subject-matter; or
 - (b) deals with more than one set of circumstances; or
 - (c) makes allegations against more than one employer; or
 - (d) makes more than one allegation against an employer; or
 - (e) for any other reason is suitable to be dealt with in separate parts—

the regulator may, if it is administratively convenient to do so, determine that any subject-matter, set of circumstances, allegation or part, as the case requires, be treated as a separate complaint.

- (2) Subject to sub-section (3), the regulator must make a determination under sub-section (1) if it is in the interest of the complainant to do so.
- (3) The regulator must not make a determination under sub-section (1) if it is likely to prejudice any attempt at conciliation of the complaint.

37. Circumstances in which regulator may decline to entertain complaint

- (1) At any time within 60 days after the day on which a complaint is lodged, the regulator may decline to entertain the complaint by notifying the complainant and the respondent in writing to that effect if the regulator considers that—
- (a) the act or practice about which the complaint has been made is not a breach of the privacy of the worker; or
 - (b) the complaint is made on behalf of a complainant by a person who is not authorised by section 32 to do so; or
 - (c) the complaint to the regulator was made more than 12 months after the complainant became aware of the act or practice; or
 - (d) the complaint is frivolous, vexatious, misconceived or lacking in substance; or

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (e) the act or practice is the subject of—
 - (i) an application under another enactment; or
 - (ii) a proceeding in a court or tribunal—
and the subject-matter of the complaint has been, or is being, dealt with adequately by that means; or
 - (f) it would be more appropriate for the act or practice to be made the subject of an application under another enactment; or
 - (g) the act or practice is subject to a code of practice under Part 3 or an authorisation under Division 2 of Part 2 and procedures available under the code or authorisation for seeking redress have not been exhausted; or
 - (h) the complainant has complained to the respondent about the act or practice and either—
 - (i) the respondent has dealt, or is dealing, adequately with the complaint; or
 - (ii) the respondent has not yet had an adequate opportunity to deal with the complaint.
- (2) A notice under sub-section (1) must state that the complainant, by notice in writing given to the regulator, may require the regulator to refer the complaint to the Tribunal for hearing under Division 6.
- (3) Within 60 days after receiving the regulator's notice declining to entertain a complaint, the complainant, by notice in writing given to the regulator, may require him or her to refer the complaint to the Tribunal for hearing under Division 6.
- (4) The regulator must comply with a notice under sub-section (3).
- (5) If the complainant does not notify the regulator under sub-section (3), the regulator may dismiss the complaint.
- (6) As soon as possible after a dismissal under sub-section (5), the regulator must, by written notice, notify the complainant and the respondent of the dismissal.
- (7) The regulator may, by notice in writing given to the complainant and the respondent, extend the period of 60 days referred to in sub-

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

section (1) by a period not exceeding 10 days if the regulator considers it necessary or desirable to do so in the interests of justice or fairness.

- (8) A complainant may take no further action under this Act in relation to the subject-matter of a complaint dismissed under this section.

38. Regulator may dismiss stale complaint

- (1) The regulator may request a complainant to provide information in relation to a complaint.
- (2) The regulator may dismiss a complaint if he or she has had no substantive response from the complainant in the period of 90 days following a request under sub-section (1).
- (3) As soon as possible after a dismissal under sub-section (2), the regulator must, by written notice, notify the complainant and the respondent of the dismissal.
- (4) A complainant may take no further action under this Act in relation to the subject-matter of a complaint dismissed under this section.

39. Acceptance of complaint

- (1) If the regulator decides to accept a complaint in whole or in part, he or she may adopt one of the following options—
- (a) if the regulator considers that it is reasonably possible that the complaint may be conciliated successfully under Division 3, the regulator may decide to conciliate the complaint; or
- (b) if the regulator—
- (i) does not consider that it is reasonably possible that the complaint may be conciliated successfully under Division 3; or
- (ii) considers that the complaint is more likely to be resolved by the making of a ruling under Division 4—
- the regulator may decide to proceed under Division 4; or
- (c) if the regulator considers that, in the circumstances of the complaint, conciliation or the making of a ruling is

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

inappropriate, he or she may decide to decline to further entertain the complaint.

- (2) Sub-section (1) does not apply to a complaint that the regulator has declined to entertain under section 37 or dismissed under section 38.
- (3) In making a decision under sub-section (1), the regulator may take into account the wishes, if expressed, of the complainant and the respondent.
- (4) The regulator must notify the complainant and the respondent in writing of his or her decision under sub-section (1).
- (5) A notice under sub-section (4) must state that the complainant, by notice in writing given to the regulator, may require the regulator to refer the complaint to the Tribunal for hearing under Division 6.

40. What happens if conciliation or ruling is inappropriate?

- (1) Within 60 days after receiving the regulator's notice under section 39(4), the complainant, by written notice, may require the regulator to refer the complaint to the Tribunal for hearing under Division 6.
- (2) The regulator must comply with a notice under sub-section (1).
- (3) If the complainant does not notify the regulator under sub-section (1), the regulator may dismiss the complaint.
- (4) As soon as possible after a dismissal under sub-section (3), the regulator must, by written notice, notify the complainant and the respondent of the dismissal.
- (5) A complainant may take no further action under this Act in relation to the subject-matter of a complaint dismissed under this section.

41. Duty to stop proceedings

- (1) The regulator must cease dealing with an issue raised in a complaint if he or she—
 - (a) becomes aware that the complainant or respondent has begun legal proceedings which relate to that issue; or
 - (b) becomes aware that proceedings relating to that issue have been initiated before a court or tribunal.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (2) Within 14 days after ceasing to deal with an issue under sub-section (1), the regulator must give written notice of the fact to the complainant and the respondent.
- (3) Despite sub-section (1), the regulator—
 - (a) may, with the consent of the complainant and the respondent, continue dealing with the issue, but only by referring it to conciliation; and
 - (b) must cease dealing with the issue when the regulator becomes aware that a court or tribunal has commenced to hear a proceeding relating to it.
- (4) If the regulator has ceased dealing with an issue raised in a complaint and later becomes aware that the complainant or the respondent has withdrawn proceedings relating to the issue, the regulator may, with the consent of the complainant, re-open proceedings under this Act.

Division 3—Conciliation of Complaints**42. Conciliation process**

- (1) If the regulator decides under section 39(1) to conciliate a complaint, he or she must make all reasonable endeavours to conciliate the complaint.
- (2) The regulator may require a party to attend conciliation either personally or by a representative who has authority to settle the matter on behalf of the party.

43. Power to obtain information and documents

- (1) If the regulator has reason to believe that a person has information or a document relevant to conciliation under this Division, the regulator may give to the person a written notice requiring the person—
 - (a) to give the information to the regulator in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or
 - (b) to produce the document to the regulator.
- (2) If the regulator has reason to believe that a person has information relevant to a conciliation under this Division, the regulator may give

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

to the person a written notice requiring the person to attend before the regulator at a time and place specified in the notice to answer questions relevant to the complaint.

44. Conciliation agreements

- (1) If, following conciliation, the parties to the complaint reach agreement with respect to the subject-matter of the complaint—
 - (a) at the request of any party made within 30 days after agreement is reached, a written record of the conciliation agreement is to be prepared by the parties or the regulator; and
 - (b) the record must be signed by or on behalf of each party and certified by the regulator; and
 - (c) the regulator must give each party a copy of the signed and certified record.
- (2) Any party, after notifying in writing the other party, may lodge a copy of the signed and certified record with the Tribunal for registration.
- (3) Subject to sub-section (4), the Tribunal must register the record and give a certified copy of the registered record to each party.
- (4) If the Tribunal, constituted by a presidential member, considers that it may not be practicable to enforce, or to supervise compliance with, a conciliation agreement, the Tribunal may refuse to register the record of the agreement.
- (5) On registration, the record must be taken to be an order of the Tribunal in accordance with its terms and may be enforced accordingly.
- (6) The refusal of the Tribunal to register the record of a conciliation agreement does not affect the validity of the agreement.

45. Conciliation statements, acts and documents inadmissible

- (1) Subject to sub-section (2), evidence of anything said or done in the course of conciliation is not admissible in proceedings before the Tribunal or any other legal proceedings relating to the subject-matter

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

of the complaint, unless all parties to the conciliation otherwise agree.

- (2) A document prepared by a party for the purpose of, or in connection with, a conciliation (or a copy of such a document), whether or not produced or used in the course of the conciliation, is not admissible in proceedings before the Tribunal or any other legal proceedings relating to the subject-matter of the complaint, unless all parties to the conciliation otherwise agree.

46. What happens if conciliation fails?

- (1) If the regulator has attempted unsuccessfully to conciliate a complaint, he or she—
 - (a) must decide whether to investigate the complaint under Division 4 or to take no further action in respect of the complaint; and
 - (b) must notify the complainant and the respondent in writing.
- (2) A notice under sub-section (1) must state that the complainant, by notice in writing given to the regulator—
 - (a) may require the regulator to refer the complaint to the Tribunal for hearing under Division 6; and
 - (b) if the regulator proposes to investigate the complaint, may object or agree to the investigation.
- (3) If the regulator proposes to take no further action in respect of a complaint, the complainant, by written notice to the regulator within 60 days after receiving the notice under sub-section (1), may require the regulator to refer the complaint to the Tribunal for hearing under Division 6.
- (4) If the regulator proposes to investigate a complaint under Division 4, the complainant, by written notice to the regulator within 60 days after receiving the notice under sub-section (1)—
 - (a) may object to the investigation and may require the regulator to refer the complaint to the Tribunal for hearing under Division 6; or
 - (b) may agree to the investigation.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (5) The regulator must comply with a notice under sub-section (3) or (4)(a).
- (6) If the complainant does not notify the regulator under sub-section (3) or (4), the regulator must dismiss the complaint.
- (7) If the complainant objects to the investigation but does not require the regulator to refer the complaint to the Tribunal for hearing under Division 6, the regulator must dismiss the complaint.
- (8) As soon as possible after a dismissal under sub-section (6) or (7), the regulator must, by written notice, notify the complainant and the respondent of the dismissal.
- (9) A complainant may take no further action under this Act in relation to the subject-matter of a complaint dismissed under this section.
- (10) If a complainant agrees to an investigation of the complaint, the regulator—
 - (a) must notify the respondent in writing that an investigation will be conducted; and
 - (b) must investigate the complaint as soon as practicable after receipt of the notice under sub-section (4)(b).

Division 4—Investigations, Rulings and Compliance Notices**47. Investigation and ruling**

- (1) The regulator may investigate—
 - (a) a complaint in respect of which he or she has made a decision under section 39(1)(b); and
 - (b) a complaint referred to in section 46(1) which he or she has decided to investigate in circumstances where the complainant has agreed to the investigation—

and make a ruling as to whether the act or practice of the respondent that is the subject of the complaint is a breach of the privacy of the complainant.

- (2) A ruling must include—
 - (a) the reasons for the ruling; and

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (b) the action, if any, that the regulator specifies to remedy the complaint; and
 - (c) the action, if any, that the regulator specifies to protect the privacy of workers other than the complainant; and
 - (d) a specified period, not exceeding 60 days, within which the action must be taken.
- (3) Within 14 days after making a ruling under sub-section (1), the regulator must serve written notice of the ruling on the complainant and the respondent.
- (4) If the regulator rules that a respondent has breached the privacy of the complainant, the regulator may require the respondent to do any or all of the following—
- (a) cease from engaging in any act or practice that is the subject of the complaint;
 - (b) take specified action to remedy the consequences of the act or practice that is the subject of the complaint or redress any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of that act or practice;
 - (c) publish, at the expense of the respondent, an advertisement in a newspaper circulating generally in Victoria containing information specified by the regulator.
 - (d) take specified action to protect the privacy of workers other than the complainant.
- (5) If the regulator rules that a respondent has breached an authorisation granted under Division 2 of Part 2 to engage in an act or practice, the regulator may revoke or amend the authorisation.
- (6) If the regulator is satisfied, on the application of an employer on which a ruling is served, that it is not reasonably possible to take the action specified in the ruling within the period specified in the ruling, the regulator may extend the period specified in the ruling on the giving to the regulator by the employer of an undertaking to take the specified action within the extended period.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (7) The regulator may only extend a period under sub-section (6) if an application for the extension is made before the period specified in the ruling expires.
- (8) A respondent who receives notice of a ruling under sub-section (3) which requires the respondent to take specified action must report in writing to the regulator, within 7 days after the expiry of the period, or extended period, within which the action must be taken, on the action taken by the respondent with respect to the ruling.
- (9) The regulator must give written notice to the complainant of the contents of a report referred to in sub-section (8) within 7 days after receipt of the report or, if the report has not been provided, must give written notice to the complainant of that fact within 7 days after the expiry of the period, or extended period, referred to in sub-section (8).

48. Referral to Tribunal

The complainant or the respondent, by written notice to the regulator within 60 days after receiving notice of a ruling with respect to a complaint under section 47(3), may require the regulator to refer the complaint to the Tribunal for hearing under Division 6.

49. Enforcement of ruling

- (1) If the respondent fails—
 - (a) to comply with a ruling; or
 - (b) to report to the regulator as required by section 47(8)—the complainant, after notifying the respondent in writing, may lodge a copy of the ruling, as notified under section 47(3), with the Tribunal for registration.
- (2) Any party, after notifying in writing the other party, may lodge a copy of the ruling, as notified under section 47(3), with the Tribunal for registration.
- (3) The Tribunal must register the ruling and give a certified copy of the ruling to each party.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (4) On registration, the ruling must be taken to be an order of the Tribunal in accordance with its terms and may be enforced accordingly.
- (5) The regulator must provide to the Tribunal a copy of all documents (including any record of evidence provided to the regulator) that were considered by the regulator in the investigation of the complaint.

Note: The regulator has powers under section 73 to determine compliance with a ruling or with a compliance notice under section 50.

50. Compliance notice

- (1) The regulator may serve a compliance notice on an employer if it appears to the regulator that—
 - (a) the employer has performed an act or engaged in a practice that is a breach of the privacy of a worker; and
 - (b) the act or practice constitutes a serious or flagrant breach.
- (2) A compliance notice requires the employer—
 - (a) to take specified action within a specified period or to refrain from taking specified action that the regulator believes to be necessary for the purpose of ensuring that the privacy of workers is not breached; and
 - (b) to report the taking of any required action to the regulator in a specified manner within a specified period after taking that action.
- (3) If the regulator is satisfied, on the application of an employer served with a compliance notice, that it is not reasonably possible to take the action specified in the notice within the period specified in the notice, the regulator may extend the period specified in the notice on the employer giving to the regulator an undertaking to take the specified action within the extended period.
- (4) The regulator may only extend a period under sub-section (3) if an application for the extension is made before the period specified in the notice expires.
- (5) The regulator may act under sub-section (1)—

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (a) on his or her own initiative at any stage and irrespective of whether a complaint has been made or a complainant has objected to an investigation; or
 - (b) on an application by a worker who was a complainant under this Part and the complaint was the subject of a conciliation or ruling or was determined by the Tribunal under Division 6.
- (6) In deciding whether or not to serve a compliance notice, the regulator may have regard to the extent to which the employer has complied with a ruling of the regulator or a decision of the Tribunal under Division 6.

51. Power to obtain information and documents

- (1) If the regulator has reason to believe that a person has information or a document relevant to an investigation or ruling under section 47 or to a decision on whether to serve a compliance notice under section 50, the regulator may give to the person a written notice requiring the person—
 - (a) to give the information to the regulator in writing signed by the person or, in the case of a body corporate, by an officer of the body corporate; or
 - (b) to produce the document to the regulator.
- (2) If the regulator has reason to believe that a person has information relevant to an investigation or ruling under section 47 or to a decision on whether to serve a compliance notice under section 50, the regulator may give to the person a written notice requiring the person to attend before the regulator at a time and place specified in the notice to answer questions relevant to the decision.

52. Power to examine witnesses

- (1) The regulator may administer an oath or affirmation to a person required to attend under section 51(2) and may examine the person on oath or affirmation.
- (2) The oath or affirmation to be taken or made by a person for the purposes of this section is an oath or affirmation that the answers the person will give will be true.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

53. Conduct of investigation etc.

In exercising a power under section 47, 50, 51 or 52, the regulator—

- (a) must proceed with as much expedition as the requirements of this Act and proper investigation of the matter permit; and
- (b) is not bound by the rules of evidence; and
- (c) may inform himself or herself in any manner that he or she thinks fit.

54. Protection against self-incrimination

It is a reasonable excuse for a natural person to refuse or fail to give information or answer a question or to produce a document when required to do so under this Part if giving the information or answering the question or producing the document might tend to incriminate the person.

55. Failure to comply with compliance notice

- (1) An employer must comply with a compliance notice served on it under section 50(1) that is in effect.
- (2) A compliance notice served under section 50(1) does not take effect until the latest of—
 - (a) the expiry of the period specified in the notice; or
 - (b) the expiry of any extended period fixed under section 50(3); or
 - (c) the expiry of the period within which an application for review of the decision to serve the notice may be made to the Tribunal under section 56(1); or
 - (d) if an application is made under section 56(1) for review of the decision to serve the notice, the affirming of the decision on the review.

56. Application for review—compliance notice

- (1) A worker or employer whose interests are affected by a decision of the regulator under section 50(1) to serve a compliance notice may apply to the Tribunal for review of the decision.

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (2) An application for review must be made within 28 days after the later of—
 - (a) the day on which the decision is made; or
 - (b) if, under the **Victorian Civil and Administrative Tribunal Act 1998**, the person requests a statement of reasons for the decision, the day on which the statement of reasons is given to the person or the person is informed under section 46(5) of that Act that a statement of reasons will not be given.
- (3) The regulator is a party to a proceeding on a review under this section.

Division 5—Interim Orders**57. Tribunal may make interim orders before hearing**

- (1) A complainant or a respondent or the regulator may apply to the Tribunal for an interim order to prevent any party to the complaint from acting in a manner prejudicial to negotiations or conciliation or to any decision or order the Tribunal might subsequently make.
- (2) An application may be made under sub-section (1) at any time before the complaint is referred to the Tribunal.
- (3) In making an interim order, the Tribunal must have regard to—
 - (a) whether or not the complaint raises a serious question; and
 - (b) any possible detriment or advantage to the public interest in making the order; and
 - (c) any possible detriment to the complainant's or the respondent's case if the order is not made.
- (4) An interim order applies for the period, not exceeding 28 days, specified in it and may be extended from time to time by the Tribunal.
- (5) The party against whom the interim order is sought is a party to the proceeding on an application under sub-section (1).
- (6) In making an interim order, the Tribunal—

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (a) may require any undertaking as to costs or damages that it considers appropriate; and
 - (b) may make provision for the lifting of the order if specified conditions are met.
- (7) The Tribunal may assess any costs or damages referred to in subsection (6)(a).
- (8) Nothing in this section affects or takes away from the Tribunal's power under section 123 of the **Victorian Civil and Administrative Tribunal Act 1998** to make orders of an interim nature in a proceeding in the Tribunal in respect of a complaint.

Division 6—Jurisdiction of the Tribunal**58. When may the Tribunal hear a complaint?**

The Tribunal may hear a complaint referred to it by the regulator under this Part.

Note: The regulator may refer complaints to the Tribunal under sections 37, 40, 46 and 48.

59. Who are the parties to a proceeding?

- (1) The complainant and the respondent are parties to a proceeding in respect of a complaint referred to the Tribunal by the regulator.
- (2) The regulator is not a party to a proceeding in respect of a complaint referred to the Tribunal by him or her unless joined by the Tribunal.

60. What may the Tribunal decide?

After hearing the evidence and representations that the parties to a complaint desire to adduce or make, the Tribunal may—

- (a) find the complaint or any part of it proven and make any one or more of the following orders—
 - (i) an order restraining the respondent, or the employer of which the respondent is the committee of management, from repeating or continuing any act or practice the subject of the complaint which the Tribunal has found to constitute a breach of the privacy of the complainant;

*Workplace Privacy Act 2005**Act No.*

Part 4—Complaints

- (ii) an order that the respondent perform or carry out any action to redress any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the act or practice that is the subject of the complaint;
 - (iii) an order that the complainant is entitled to a specified amount, not exceeding \$100 000, by way of compensation for any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the act or practice the subject of the complaint;
 - (iv) an order revoking an authorisation granted to the respondent, or the employer of which the respondent is the committee of management, by the regulator under Division 2 of Part 2;
 - (v) an order that the employer publish, at the expense of the employer, an advertisement in a newspaper circulating generally in Victoria containing information specified in the order; or
- (b) find the complaint or any part of it proven but decline to take any further action in the matter; or
 - (c) find the complaint or any part of it not proven and make an order that the complaint or part be dismissed; or
 - (d) in any case, make an order that the complainant is entitled to a specified amount to reimburse the complainant for expenses reasonably incurred by the complainant in connection with the making of the complaint and the proceedings held in respect of it under this Act; or
 - (e) in any case, make an order that the respondent take specified action to protect the privacy of workers other than the complainant.
-

Workplace Privacy Act 2005
Act No.
Part 5—Other Investigations and Inquiries

PART 5—OTHER INVESTIGATIONS AND INQUIRIES

Division 1—Investigations Initiated by the Regulator

61. When can the regulator initiate an investigation?

If, in the course of dealing with a complaint under Part 4, the regulator becomes aware of circumstances where a contravention of this Act may have occurred (other than the contravention alleged in the complaint or the contravention being investigated), the regulator may investigate those circumstances.

62. Conduct of investigation

- (1) The regulator is to conduct an investigation under section 61 in the same manner, as nearly as practicable, as if it were a complaint.
- (2) The regulator must, as soon as practicable, give written notice of the investigation to the employer concerned.
- (3) Division 4 of Part 4 and Part 6 apply to an investigation under section 61 as if—
 - (a) a reference to a respondent were a reference to the employer under investigation; and
 - (b) a reference to a complainant were a reference to the regulator; and
 - (c) a reference to a complaint were a reference to the matter being investigated.
- (4) The regulator may investigate any matter referred to in section 61 and make a ruling in accordance with section 47 as to whether the act or practice of the employer that is the subject of the investigation is a breach of the privacy of one or more workers.
- (5) Within 14 days after making a ruling under sub-section (4), the regulator must serve written notice of the ruling on the employer concerned in accordance with section 47.

Note: The regulator has powers under section 73 to determine compliance with a ruling or a compliance notice under section 50 as applied to an investigation under section 61.

*Workplace Privacy Act 2005**Act No.*

Part 5—Other Investigations and Inquiries

63. Powers in conducting an investigation

In exercising a power conferred by section 47, 50, 51 or 52 (as applied to an investigation under section 61 by section 62(3)), the regulator—

- (a) must proceed with as much expedition as the requirements of this Act and proper investigation of the matter permit; and
- (b) is not bound by the rules of evidence; and
- (c) may inform himself or herself in any manner that the regulator thinks fit.

64. Protection against self-incrimination

It is a reasonable excuse for a natural person to refuse or fail to give information or answer a question or to produce a document when required to do so under this Part if giving the information or answering the question or producing the document might tend to incriminate the person.

65. Referral to Tribunal

- (1) An employer, by written notice within 60 days after receiving notice of a ruling under section 62(4), may require the regulator to refer the matter to the Tribunal for hearing under Division 6.
- (2) The regulator—
 - (a) must comply with a notice under sub-section (1); and
 - (b) must provide to the Tribunal a copy of all documents that were considered by the regulator in the investigation.

66. Order by the Tribunal

If a matter has been referred to the Tribunal under section 65, the Tribunal must conduct an inquiry into the matter and, if satisfied that an employer has breached the privacy of a worker, may make any order referred to in section 60 with any necessary modification.

Workplace Privacy Act 2005
Act No.
Part 5—Other Investigations and Inquiries

Division 2—Inquiries Undertaken by the Regulator

67. When can the regulator initiate an inquiry?

- (1) The regulator may inquire into any act or practice that may be inconsistent with or contrary to this Act.
- (2) If—
 - (a) the regulator is of the opinion that the act or practice is inconsistent with or contrary to this Act; and
 - (b) the regulator has not considered it appropriate to endeavour to effect settlement of the matters that gave rise to the inquiry or has endeavoured without success to effect a settlement—the regulator may report to the Minister in relation to the inquiry.

68. Conduct of inquiry

- (1) The regulator may conduct an inquiry under section 67 in any manner that he or she thinks fit and, in informing himself or herself in the course of an inquiry, is not bound by the rules of evidence.
- (2) For the purposes of the performance of his or her functions, the regulator may work with and consult appropriate persons, governmental organisations and non-governmental organisations.

69. Power to obtain information and documents and power to examine witnesses

Sections 51 and 52 apply to an inquiry under this Division as if a reference to a decision under section 47 or 50 were a reference to an inquiry under this Division.

70. Regulator to give opportunity for making submissions

If it appears to the regulator as a result of an inquiry into an act or practice that the act or practice is inconsistent with or contrary to this Act, the regulator must not provide a report to the Minister in relation to the act or practice until the regulator has given a reasonable opportunity to the person who did the act or engaged in the practice to do either or both of the following—

*Workplace Privacy Act 2005**Act No.*

Part 5—Other Investigations and Inquiries

- (a) appear before the regulator, whether in person or by a representative, and make oral submissions in relation to the act or practice;
- (b) make written submissions to the regulator in relation to the act or practice.

71. Report to contain recommendations

If, after an inquiry into an act done or practice engaged in by a person, the regulator finds that the act or practice is inconsistent with or contrary to this Act, the regulator—

- (a) must give notice in writing to the person setting out the findings of the regulator and the reasons for those findings; and
- (b) may include in the notice any recommendations by the regulator for preventing a repetition of the act or a continuation of the practice; and
- (c) must include in any report to the Minister relating to the results of the inquiry particulars of any recommendations that the regulator has made under paragraph (b); and
- (d) must state in that report whether, to the knowledge of the regulator, the person has taken or is taking any action as a result of the findings, and recommendations, if any, of the regulator and, if the person has taken or is taking any action, the nature of that action.

72. Reports to be tabled in Parliament

The Minister must cause any report provided to him or her by the regulator under this Division to be laid before each House of the Parliament within 15 sitting days of that House after the report is received by the Minister.

*Workplace Privacy Act 2005**Act No.*

Part 6—Power to View Premises and Systems

PART 6—POWER TO VIEW PREMISES AND SYSTEMS**73. Searches to monitor compliance with Act**

- (1) To the extent that it is reasonably necessary to do so for the purpose of determining compliance with a ruling made under section 47 or 62 or with a compliance notice served under section 50, the regulator may exercise powers under this section.
- (2) Subject to this section, the regulator may enter, at any time during ordinary working hours on any business day, any premises that the regulator believes on reasonable grounds are premises where a work-related activity is taking place and may do any one or more of the following—
 - (a) inspect and take photographs (including video recordings), or make sketches or other records, of the premises or of any thing at the premises or of any activity taking place at the premises;
 - (b) inspect, and make copies of, or take extracts from, any document kept at the premises.
- (3) The regulator may not exercise any powers under this section if the regulator fails to produce, on request, his or her identity card for inspection by the occupier of the premises.
- (4) The regulator may not, under this section, enter a residence unless the occupier of the residence has consented in writing to the entry and the inspection.

74. Operation of electronic equipment at premises

- (1) If—
 - (a) a thing found at premises that the regulator has entered under section 73 is or includes a disk, tape or other device for storage of information; and
 - (b) equipment at the premises may be used with the disk, tape or other storage device; and
 - (c) the regulator believes on reasonable grounds that the information stored on the disk, tape or other storage device is

*Workplace Privacy Act 2005**Act No.*

Part 6—Power to View Premises and Systems

relevant to determine whether this Act has been complied with—

the regulator may require the employer or a worker of the employer to operate the equipment to access the information.

- (2) In exercising a power under this section, the regulator must, insofar as is reasonably practicable, minimise the effect of the exercise of the power on the running of the employer's business.

75. Power to require information or documents

If the regulator—

- (a) exercises a power of entry under this Part; and
- (b) produces his or her identity card for inspection by a person—

the regulator may, to the extent that it is reasonably necessary to determine compliance with this Act, require the person to give information to the regulator, to produce documents to the regulator and to give reasonable assistance to the regulator.

76. Protection against self-incrimination

It is a reasonable excuse for a natural person to refuse or fail to give information, produce a document or do any other thing that the person is required to do under this Part, if the giving of the information, the production of the document or the doing of that other thing would tend to incriminate the person.

Workplace Privacy Act 2005
Act No.
Part 7—Enforcement

PART 7—ENFORCEMENT

Division 1—Civil Penalties

77. Conduct attracting civil penalties

- (1) An employer must comply with—
 - (a) section 9(1);
 - (b) section 10;
 - (c) section 12;
 - (d) section 47(8);
 - (e) section 47(8) as applied by section 62(4).
- (2) An employer must comply with a compliance notice served under section 50(1) that is in effect within the meaning of section 55.

78. Proceedings for contravention of civil penalty provision

- (1) The regulator may apply to the Magistrates' Court for an order that an employer pay a pecuniary penalty for a contravention by the employer of a civil penalty provision.
- (2) If the Magistrates' Court is satisfied on the balance of probabilities that an employer has contravened a civil penalty provision, the Court may order the employer to pay a pecuniary penalty to the Minister in respect of each act or omission by the employer to which this section applies, being an amount—
 - (a) in the case of a civil penalty provision referred to in section 77(1)(d) or (e), of \$1000; and
 - (b) in any other case, not exceeding \$300 000 in the case of a body corporate, or \$60 000 in any other case.
- (3) In determining the amount of the pecuniary penalty to be paid by an employer, the Magistrates' Court must have regard to all relevant matters including—
 - (a) the nature and extent of the act or omission; and

*Workplace Privacy Act 2005**Act No.*

Part 7—Enforcement

- (b) the nature and extent of any loss or damage suffered as a result of the act or omission; and
 - (c) the circumstances in which the act or omission took place; and
 - (d) whether the employer has previously been found by the Court in proceedings under this section to have contravened a civil penalty provision.
- (4) For the purposes of determining the penalty for a contravention of a civil penalty provision, if the contravention consists of a failure to do something that is required to be done, the contravention is to be regarded as continuing until the act is done.
- (5) The Magistrates' Court may grant an injunction requiring an employer to cease contravening a civil penalty provision.
- (6) A contravention of a civil penalty provision is not an offence.

79. Conduct in contravention of more than one civil penalty provision

If the act or omission of an employer constitutes a contravention of 2 or more civil penalty provisions, proceedings may be instituted under section 78 against the employer in relation to either or any or all of those provisions, but the employer is not liable to be punished more than once for the same act or omission.

80. Application and enforcement of civil penalties

- (1) Every pecuniary penalty received by the Minister must be paid into the Consolidated Fund.
- (2) A pecuniary penalty ordered to be paid under section 78 may be recovered in a court of competent jurisdiction as a debt due to the Crown.

Division 2—Criminal penalties**81. Failure to attend etc. before regulator**

A person must not, without reasonable excuse—

- (a) refuse or fail—
 - (i) to attend before the regulator; or
 - (ii) to be sworn or make an affirmation; or

*Workplace Privacy Act 2005**Act No.*

Part 7—Enforcement

- (iii) to give information; or
- (iv) to answer a question or produce a document; or
- (v) to give reasonable assistance—
when so required by the regulator under this Act; or
- (b) wilfully obstruct, hinder or resist the regulator or a person authorised by the regulator under this Act in—
 - (i) performing, or attempting to perform, a function or duty under this Act; or
 - (ii) exercising, or attempting to exercise, a power under this Act; or
- (c) furnish information or make a statement to the regulator knowing that it is false or misleading in a material particular; or
- (d) produce a document that the person knows to be false or misleading in a material particular without indicating the respect in which it is false or misleading and, if practicable, providing correct information.

Penalty: 60 penalty units.

82. Secrecy

- (1) This section applies to a person who is, or has been, the regulator, an acting regulator, a delegate of the regulator, a person employed for the purposes of this Act, a person authorised by the regulator or a consultant engaged by the regulator.
- (2) A person to whom this section applies must not, directly or indirectly, make a record of, disclose or communicate to any person any information relating to the affairs of any person or body acquired in the performance of functions or duties or the exercise of powers under this Act unless—
 - (a) it is necessary to do so for the purposes of, or in connection with, the performance of a function or duty or the exercise of a power under this Act; or

*Workplace Privacy Act 2005**Act No.*

Part 7—Enforcement

- (b) the person or body to whom the information relates gives written consent to the making of the record, disclosure or communication.

Penalty: 60 penalty units.

- (3) Without limiting sub-section (2), the regulator must not disclose or communicate to any person, other than a person employed for the purposes of this Act, any information given to the regulator in accordance with a requirement made under Division 3 or 4 of Part 4 or Part 5 (including information contained in a document required to be produced to the regulator) unless the regulator—
 - (a) has notified the person from whom the information was obtained of the proposal to disclose or communicate that information; and
 - (b) has given that person a reasonable opportunity to object to the disclosure or communication.

Penalty: 60 penalty units.

83. Offences by bodies

If this Act provides that a body is guilty of an offence, that reference to a body must, if the body is unincorporated, be read as a reference to each member of the committee of management of the body.

84. Prosecutions

- (1) A proceeding for an offence against this Act may be brought by—
 - (a) a member of the police force; or
 - (b) the regulator; or
 - (c) a person authorised to do so, either generally or in a particular case, by the regulator.
- (2) In a proceeding for an offence against this Act, it must be presumed, in the absence of evidence to the contrary, that the person bringing the proceeding was authorised to bring it.

*Workplace Privacy Act 2005**Act No.*

Part 7—Enforcement

Division 3—Employees and Agents**85. Employees and agents**

- (1) Any act done or practice engaged in on behalf of an employer by an employee or agent of the employer acting within the scope of his or her actual or apparent authority is to be taken, for the purposes of this Act including a prosecution for an offence against this Act, to have been done or engaged in by the employer and not by the employee or agent unless the employer establishes that the employer took reasonable precautions and exercised due diligence to avoid the act being done or the practice being engaged in by the employee or agent.
 - (2) If, for the purpose of investigating a complaint or a proceeding for an offence against this Act, it is necessary to establish the state of mind of an employer in relation to a particular act or practice, it is sufficient to show—
 - (a) that the act was done or practice engaged in by an employee or agent of the employer acting within the scope of his or her actual or apparent authority; and
 - (b) that the employee or agent had that state of mind.
-

*Workplace Privacy Act 2005**Act No.*

Part 8—General

PART 8—GENERAL**Division 1—The Regulator****86. Appointment of the regulator**

- (1) The Governor in Council may appoint a person as the regulator.
- (2) A person who is a member of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory cannot be appointed under sub-section (1).

Note: The Privacy Commissioner is the regulator if no appointment is made under this section.

87. Remuneration and allowances

The regulator, if appointed under section 86(1), is entitled to be paid the remuneration and allowances that are determined by the Governor in Council.

88. Terms and conditions of appointment

- (1) This section applies if the regulator is appointed under section 86(1).
- (2) Subject to this Part, the regulator holds office for the period, not exceeding 7 years, that is specified in the instrument of appointment but is eligible for re-appointment.
- (3) Subject to this Part, the regulator holds office on the terms and conditions determined by the Governor in Council.
- (4) The regulator is entitled to leave of absence as determined by the Governor in Council.
- (5) The regulator must not engage, directly or indirectly, in paid employment outside the duties of regulator.
- (6) The **Public Administration Act 2004** (other than Part 2) does not apply to the regulator in respect of the office of regulator, except as provided in section 16 of that Act.

89. Vacancy, resignation

- (1) This section applies if the regulator is appointed under section 86(1).

*Workplace Privacy Act 2005**Act No.*

Part 8—General

- (2) The regulator ceases to hold office if he or she—
 - (a) is convicted of an indictable offence or an offence which, if committed in Victoria, would be an indictable offence; or
 - (b) nominates for election for either House of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory.
- (3) The regulator may resign by notice in writing delivered to the Governor in Council.

90. Suspension of the regulator

- (1) This section applies if the regulator is appointed under section 86(1).
- (2) The Governor in Council may suspend the regulator from office.
- (3) The Minister must cause to be laid before each House of Parliament a full statement of the grounds of suspension within 7 sitting days of that House after the suspension.
- (4) The regulator must be removed from office by the Governor in Council if each House of Parliament within 20 sitting days after the day when the statement is laid before it declares by resolution that the regulator ought to be removed from office.
- (5) The Governor in Council must remove the suspension and restore the regulator to office unless each House makes a declaration of the kind specified in sub-section (4) within the time specified in that sub-section.

91. Acting appointment

- (1) The Governor in Council may appoint a person to act in the office of regulator during a period or all periods when the regulator, if appointed under section 86(1), is absent from duty or is, for any reason, unable to perform the duties of the office.
- (2) An appointment under sub-section (1) is for the period, not exceeding 6 months, that is specified in the instrument of appointment.
- (3) A person is not eligible to be appointed under sub-section (1) if the person is a member of the Parliament of Victoria or of the Commonwealth or of any other State or a Territory.

*Workplace Privacy Act 2005**Act No.*

Part 8—General

- (4) The Governor in Council may at any time remove the acting regulator from office.
- (5) While a person is acting in the office of the regulator in accordance with this section, the person—
 - (a) has, and may exercise, all the powers and must perform all the duties of that office under this Act; and
 - (b) is entitled to be paid the remuneration and allowances that the regulator would have been entitled to for performing those duties.

92. Validity of acts and decisions

An act or decision of the regulator or acting regulator is not invalid only because—

- (a) of a defect or irregularity in or in connection with his or her appointment; or
- (b) in the case of an acting regulator, that the occasion for so acting had not arisen or had ceased.

93. Staff

- (1) There may be employed under Part 3 of the **Public Administration Act 2004** any employees that are necessary for the purposes of this Act.
- (2) The regulator may engage as many consultants as are required for the exercise of his or her functions.

94. Functions of the regulator

In addition to any other functions conferred on him or her by or under this Act, the regulator has the following functions—

- (a) to promote understanding and acceptance of the requirements of this Act;
- (b) to advise the Minister on any enactment or proposed enactment that may adversely affect the privacy of workers or contravene this Act;

*Workplace Privacy Act 2005**Act No.*

Part 8—General

- (c) to conduct audits of an employer for the purpose of ascertaining whether the employer is complying with this Act and any applicable code of practice;
- (d) to issue guidelines on the operation of this Act;
- (e) to provide educational programs for the purpose of promoting understanding of how this Act operates and generally to promote public awareness of its objects and purposes;
- (f) to monitor and report on equipment and systems that are intended to minimise the impact of acts or practices affecting the privacy of workers;
- (g) to undertake research into and monitor developments affecting workplace privacy.

95. Powers of the regulator

Subject to this Act, the regulator has the power to do all things that are necessary or convenient to be done for or in connection with the performance of the functions of the regulator.

96. Immunity of regulator

- (1) The regulator is not personally liable for anything done or omitted to be done in good faith—
 - (a) in the exercise of a power or discharge of a duty under this Act or the regulations; or
 - (b) in the reasonable belief that the act or omission was in the exercise of a power or the discharge of a duty under this Act or the regulations.
- (2) Any liability resulting from an act or omission that would, but for sub-section (1), attach to the regulator attaches to the State.

97. Delegation

The regulator may, by instrument, delegate to a person employed for the purposes of this Act, or a person belonging to a class of those persons, any of the powers of the regulator under this Act other than this power of delegation.

*Workplace Privacy Act 2005**Act No.*

Part 8—General

98. Annual report

The regulator must provide to the Minister for inclusion in the annual report of operations under Part 7 of the **Financial Management Act 1994** a report containing the following information—

- (a) the number of complaints made to the regulator during the period of the report;
- (b) the manner in which those complaints were resolved;
- (c) the number of investigations initiated by the regulator during the period of the report;
- (d) any other information concerning complaints that the regulator thinks fit to report;
- (e) the number of authorisations granted by the regulator during the period of the report and the purpose for which they were granted;
- (f) the number of times during the period of the report that the regulator exercised a power under Part 6.

99. Other reports

- (1) In addition to the report of operations under Part 7 of the **Financial Management Act 1994**, the regulator may report to the Minister on any act or practice that the regulator considers to be an interference with the privacy of workers or prospective workers, whether or not a complaint has been made.
- (2) The Minister must cause a copy of a report referred to in sub-section (1) to be laid before each House of the Parliament.

Division 2—Victimisation**100. Victimisation of worker**

- (1) An employer must not victimise a worker.
- (2) Without limiting sub-section (1), an employer victimises a worker if—

*Workplace Privacy Act 2005**Act No.*

Part 8—General

- (a) the employer subjects, or threatens to subject, the worker to a detriment because the worker, or a person associated with the worker—
 - (i) has made a complaint against an employer under this Act;
or
 - (ii) has given evidence or provided information or produced a document in or in connection with a proceeding under this Act; or
 - (iii) has attended a conciliation conference or done any other thing under this Act; or
 - (iv) has alleged that the employer has contravened this Act, except if the allegation is false and not made in good faith;
or
 - (v) has refused to do anything that would contravene this Act;
or
 - (b) the worker has reasonable cause to believe that the employer has subjected, or will subject, the worker to a detriment for a reason referred to in paragraph (a).
- (3) For the purposes of sub-section (2)(a)(iv), it is sufficient if the allegation states the act or omission that constitutes the contravention without stating that this Act has been contravened.
 - (4) In determining whether an employer has contravened sub-section (1), it is irrelevant—
 - (a) whether or not a factor in sub-section (2) is the only or dominant reason for the treatment or threatened treatment as long as it is a substantial reason;
 - (b) whether the employer acted alone or in association with any other person.
 - (5) A worker who claims that an employer has contravened sub-section (1) in relation to him or her may complain to the regulator.
 - (6) Part 4 applies to a complaint under sub-section (5) as if a reference to an act or practice that may be a breach of the privacy of the worker

*Workplace Privacy Act 2005**Act No.*

Part 8—General

were a reference to a contravention of sub-section (1) in relation to the worker.

(7) In this section, "**detriment**" includes humiliation and denigration.

Division 3—Regulations**101. Regulations**

The Governor in Council may make regulations for or with respect to any matter or thing required or permitted by this Act to be prescribed or necessary to be prescribed to give effect to this Act.

Division 4—Amendment of Acts**102. Amendment of Victorian Civil and Administrative Tribunal Act 1998**

At the end of Schedule 1 to the **Victorian Civil and Administrative Tribunal Act 1998** insert—

"PART 24—WORKPLACE PRIVACY ACT 2005**103. Regulator may intervene**

The regulator may intervene at any time in a proceeding under the **Workplace Privacy Act 2005**."

103. Amendment of Public Administration Act 2004

After section 16(1)(i) of the **Public Administration Act 2004** insert—

"(ia) the regulator within the meaning of the **Workplace Privacy Act 2005** in relation to the office of the regulator;".

Bibliography

Australian Bureau of Statistics, *Locations of Work*, Catalogue No 6275.0 (2000)

Employee Earnings, Benefits and Trade Union Membership, Catalogue No 6310.0 (2004)

Australian Law Reform Commission, *Privacy*, Report No 22 (1983)

Essentially Yours: The Protection of Human Genetic Information in Australia, Volume 1, Report No 96 (2003)

Essentially Yours: The Protection of Human Genetic Information in Australia, Volume 2, Report No 96 (2003)

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

Braithwaite, John, 'Responsive Business Regulatory Institutions' in CAJ Coady and CJG Sampford (eds) *Business Ethics and the Law* (Federation Press, 1993)

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11*, opened for signature 11 May 1994, ETS 005 (entered into force 1 November 1998), <www.conventions.coe.int/treaty/en/treaties/html/005.htm> at 3 August 2005

Craig, John, *Privacy and Employment Law* (Hart Publishing, 1999)

Department of Justice, *New Directions for the Victorian Justice System 2004–2014: Attorney-General's Justice Statement* (2004)

Department of Justice Strategic Priorities 2005: A Framework for Planning and Opportunities for Collaboration (2005)

- Department of Treasury and Finance, *Victorian Guide to Regulation* (2005)
- Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments* (Washington, 2003)
- European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data* (2002)
- European Commission Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context*, DG MARKT 5062/01 (entered into force 13 September 2001)
- Working Document on the Surveillance of Electronic Communications in the Workplace*, DG MARKT/5401/01 (entered into force 29 May 2002)
- Fisse, Brent and Braithwaite, John, *The Impact of Publicity on Corporate Offenders* (State University of New York Press, 1983)
- Fleming, John, *The Law of Torts* (9th ed, LBC Information Services, 1998)
- Foord, Kate, *Defining Privacy* (Victorian Law Reform Commission, 2002)
- Haines, Fiona, *Corporate Regulation: Beyond Punish or Persuade* (Clarendon Press, 1997)
- Harmsworth, Peter, 'State Services Authority: Overview' (Paper presented at the Statutory Entities Forum, Melbourne, 20 July 2005)
- 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, Sydney, 5 December 2002)
- Information and Privacy Commissioner [Ontario] *Workplace Privacy: A Consultation Paper* (1992)

- Workplace Privacy: The Need for a Safety-Net* (1993)
- Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office* (2001)
- Information Commissioner's Office [UK], *Data Protection: The Employment Practices Code* (2005)
- International Labour Office, *Management of Alcohol- and Drug-Related Issues in the Workplace: an ILO Code of Practice* (1996)
- Protection of Workers' Personal Data: An ILO Code of Practice* (1997)
- Johnston, Anna and Cheng, Myra, 'Electronic Workplace Surveillance, Part 2: Responses to Electronic Workplace Surveillance—Resistance and Regulation' (2003) 9 (10) *Privacy Law & Policy Reporter* 187
- Lebihan, Rachel, 'Privacy Law Falling Behind, Inquiry Told', *Australian Financial Review*, 7 March 2005, 13
- Maxwell, Chris, *Occupational Health and Safety Act Review* (State of Victoria, 2004)
- Morris, Caroline, 'Drugs, the Law, and Technology: Posing Some Problems in the Workplace' (2002) 20 *New Zealand Universities Law Review* 1
- National Alternative Dispute Resolution Advisory Council, 'Resolving Customer Disputes: Case Studies and Current Issues' (Panel discussion at the ADR—A Better Way to do Business conference, Sydney, 4–5 September 2003) <www.ag.gov.au> at 8 August 2005
- National Economic Research Associates, *Alternative Approaches to 'Light-Handed' Regulation: A Report for the Essential Services Commission Victoria* (2004)
- New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No 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 Butt, Peter (eds), *Butterworths Australian Legal Dictionary* (Butterworths, 1997)
- Office of the Privacy Commissioner [Aus], *Guidelines on Workplace E-mail, Web Browsing and Privacy* (30 March 2000) <www.privacy.gov.au> at 21 July 2005
- The Operation of the Privacy Act: Annual Report: 1 July 1999–30 June 2000* (2000)
- Guidelines to the National Privacy Principles* (September 2001) <www.privacy.gov.au> at 16 August 2005
- Guidelines on Privacy in the Private Health Sector* (November 2001) <www.privacy.gov.au> at 16 August 2005
- Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005)
- Office of the Privacy Commissioner for Personal Data [Hong Kong] *Code of Practice on Human Resource Management* (2000)
- Office of the Victorian Privacy Commissioner, *Annual Report 2003–04* (2004)
- Otlowski, Margaret, *Implications of Genetic Testing for Australian Employment Law and Practice*, Occasional Paper 2 (Centre for Law and Genetics, University of Tasmania Law School, 2001)
- Parker, Christine, 'Reinventing Regulation within the Corporation: Compliance-Oriented Regulatory Innovation' (2000) 32 (5) *Administration and Society* 529
- Pittard, Marilyn, 'The Dispersing and Transformed Workplace: Labour Law and the Effect of Electronic Work' (2003) 16 (1) *Australian Journal of Labour Law* 69

- Privacy Committee of New South Wales, *Drug Testing in the Workplace*, Report No 64 (1992)
- Invisible Eyes: Report on Video Surveillance in the Workplace*, Report No 67 (1995)
- Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Development* (2004) <www.privacyinternational.org/survey/> at 15 August 2005
- Public Accounts and Estimates Committee, Parliament of Victoria, *Report on the Inquiry into Corporate Governance in the Victorian Public Sector*, 63rd Report to the Parliament (2005)
- Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (Office of the Privacy Commissioner, 2004)
- Saul, Peter, 'Psychological Testing in the Selection Process' (1980) 6 (2) *Work and People* 19
- Smith, Fiona, 'Independence and Governance: One Perspective' (Paper presented at the Statutory Entities Forum, Melbourne, 20 July 2005)
- United Nations, *Universal Declaration of Human Rights*, UN GA Res 217A (III), UN GAOR 3rd sess, UN Doc A/810 at 71 (entered into force 10 December 1948), <www.un.org/Overview/rights.html> at 3 August 2005
- International Covenant on Civil and Political Rights*, GA Res 2200A (XXI), UN GAOR, 21st sess, UN Doc A/6316 (1966), 999 UNTS 171 (entered into force 23 March 1976) <www.austlii.edu.au/au/other/dfat/treaties/1980/23.html> at 3 August 2005
- Convention on the Rights of the Child*, UN Res 44/25, UN GAOR, 44th sess, UN Doc A/44/736 (entered into force 2 September 1990) <www.austlii.edu.au/au/other/dfat/treaties/1991/4.html> at 3 August 2005
- Victorian Law Reform Commission, *Privacy Law: Options for Reform—Information Paper* (2001)

Workplace Privacy: Issues Paper (2002)

Workplace Privacy: Options Paper (2004)

Waldron, Jeremy (ed), *Theories of Rights* (Oxford University Press, 1984)

Wilson, Beth, 'Health Disputes: A "Window of Opportunity" to Improve Health Services' in Ian Freckelton and Kerry Petersen (eds) *Controversies in Health Law* (Federation Press, 1999)

WorkSafe Victoria and Job Watch, *Workplace Violence and Bullying: Your Rights, What to Do, and Where to Go for Help* (2005)

World Anti-Doping Agency, *World Anti-Doping Code* (Canada, 2003)

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)

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)

Workplace Privacy: Issues Paper by Kate Foord (October 2002)

Defining Privacy: Occasional Paper (October 2002)

Sexual Offences: Interim Report (June 2003)

Defences to Homicide: Options Paper (September 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)

Workplace Privacy: Options Paper (September 2004)

Defences to Homicide: Final Report (October 2004)

Review of Family Violence Laws: Consultation Paper (November 2004)

Review of the Laws of Evidence: Information Paper (February 2005)

Assisted Reproductive Technology & Adoption: Position Paper One: Access (May 2005)

Assisted Reproductive Technology & Adoption: Position Paper Two: Parentage (July 2005)