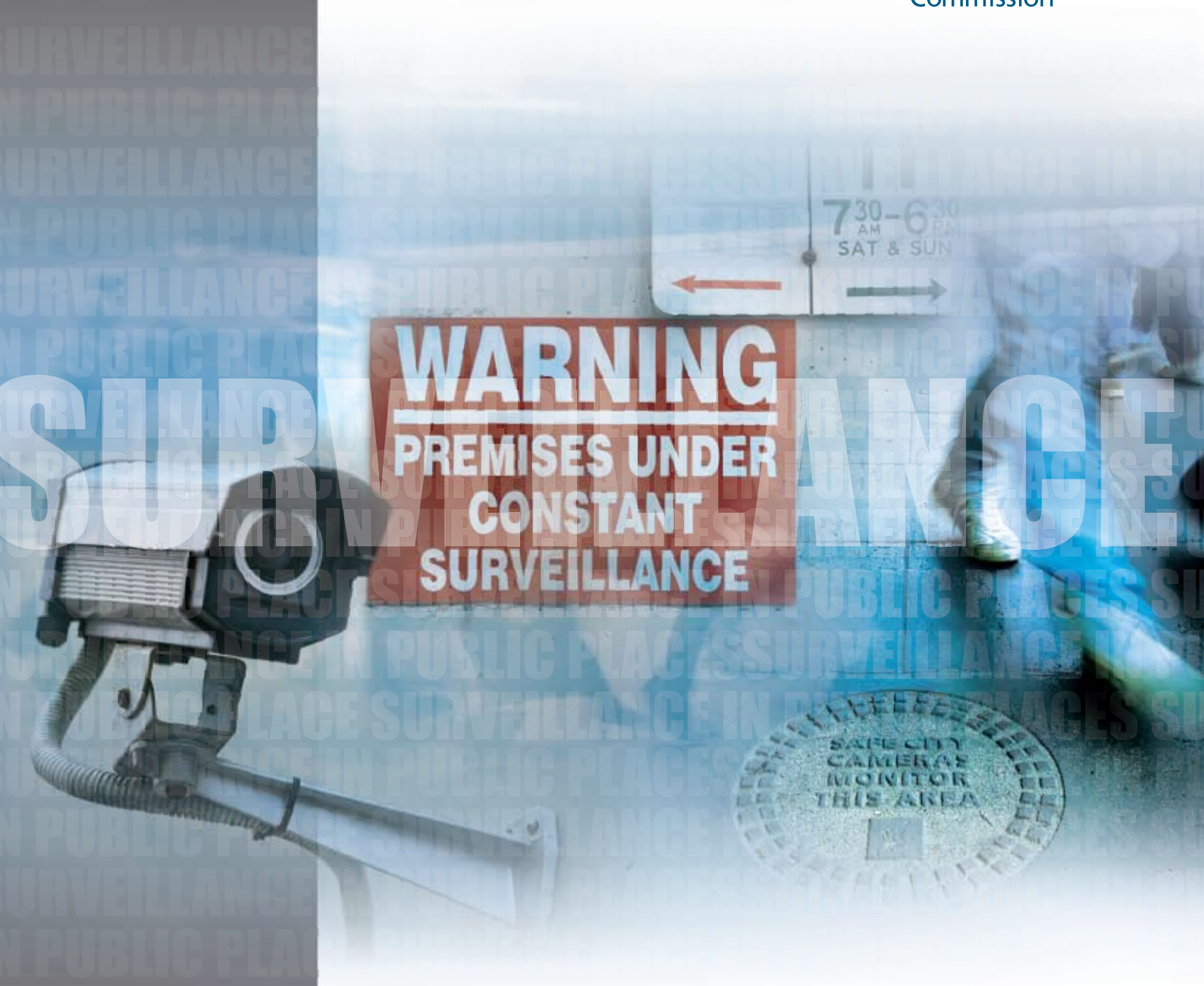
Victorian
Law Reform
Commission



SURVEILLANCE IN PUBLIC PLACES

Consultation Paper

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 January 2009.

Copyright January 2009 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 Citation* (2nd ed, 2002).

Photographs by Peter Glenane

National Library of Australia
Cataloguing-in-Publication
Victorian Law Reform Commission
Surveillance in Public Places: Consultation Paper

ISBN 9780975846636 (pbk)
1. Electronic surveillance - Social aspects - Victoria
2. Electronic surveillance - Law and legislation - Victoria
3. Public spaces - Law and legislation - Victoria
4. Privacy, Right of - Victoria

621.38928

This publication can be provided in accessible formats by contacting the commission.

Victorian
Law Reform
Commission

SURVEILLANCE IN PUBLIC PLACES

Consultation Paper 7

Victorian Law Reform Commission

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

Level 3, 333 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

Contents

Contributors

CURRENT REFERENCE TEAM

Emma Cashen (Team Leader)
Emily Minter
Lara Rabiee

VICTORIAN LAW REFORM COMMISSION

Chairperson
Professor Neil Rees

Part-time Commissioners
Paris Aristotle AM
Magistrate Mandy Chambers
Hugh de Kretser
Her Honour Judge Felicity Hampel
Professor Sam Ricketson
His Honour Judge Iain Ross AO

Chief Executive Officer
Padma Raman

Operations Manager
Kathy Karlevski

Policy and Research Team Leader
Emma Cashen

Communications Manager
Sally Finlay

Communications Officer
Clare Chandler

Policy and Research Officers
Emily Minter
Lara Rabiee
Tanaya Roy
Rupert Watters

Research Assistant
Miriam Cullen

Librarian
Julie Bransden

Project Officer
Simone Marrocco

Administrative Officers
Vicki Christou
Failelei Siatua

Contents

Preface

Surveillance in public places affects all Victorians whether we are shopping, catching public transport, driving on major roads, or attending a sporting event. This reference provides us with an opportunity to reflect upon how technological developments have changed the practice of surveillance and to assess whether our current laws are adequate.

This Consultation Paper explains how surveillance is used in public places and how it is regulated. It contains a discussion of privacy theory in the context of public places and also examines the risk and benefits of public place surveillance.

Finally, this paper contains some proposals for reform and asks a series of questions to gain feedback from the community which will inform the commission's final report.

The Attorney-General asked the commission to consider the interests of users of surveillance in protecting property and providing safe places, and to balance these against the protection of privacy, autonomy and the dignity of individuals.

The commission has been guided by these concerns and this Consultation Paper reflects the diversity of opinion and experience regarding surveillance in public places.

Two other bodies are also investigating surveillance practices in public places and contemplating reform of the law. In February 2009 the House of Lords Select Committee on the Constitution published its report titled *Surveillance: Citizens and the State*. This is the report of an inquiry into the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State.

The New Zealand Law Reform Commission released an Issues Paper that considers surveillance practices titled, *Invasion of Privacy: Penalties and Remedies,* Issues Paper 14 (2009) while this Consultation Paper was in the final stages of completion.

A related publication was released in August last year by the Australian Law Reform Commission. *For Your Information: Australian Privacy Law and Practice* is an extensive report which is of considerable relevance to this project. The timing of the Consultation Paper was delayed to ensure proper consideration of that report.

The team allocated to this project have produced high quality work. Associate Professor Moira Paterson from Monash University has played a major role in her capacity as a consultant to the commission. Team leader Emma Cashen demonstrated exceptional organisation skills. She was ably supported by Lara Rabiee and Emily Minter who are responsible for much of the paper. Priya SaratChandran, Michelle Burrell, and Bronwen Jennings provided early research and writing assistance. Additional research assistance was provided by Miriam Cullen and Suzanne Zhou. The publication was edited by Sally Finlay and produced by Clare Chandler.

The division of the commission responsible for this reference—Judge Iain Ross AO, Professor Sam Ricketson, Paris Aristotle AM and Hugh de Kretser—have provided invaluable guidance.

The object of this paper is to promote informed community debate about a challenging topic. I encourage those people and organisations with an interest in the use surveillance in public places to make a submission to the commission by 30 June 2009.

Professor Neil Rees

Chairperson

Call for Submissions

The Victorian Law Reform Commission invites your comments on this Consultation Paper.

What is a submission?

Submissions are your ideas or opinions about the law being reviewed. Submissions can be anything from a personal story about how the law has affected you, to a research paper complete with footnotes and bibliography.

The commission wants to hear from anyone who has experience with a law under review. It does not matter if you only have one or two points to make; we still want to hear from you.

What is my submission used for?

Submissions help the commission understand different views and experiences about the law it is researching. Information in submissions, along with other research and comments from meetings, is used to help develop recommendations.

Once the commission has assessed your submission it will be made available on our website and stored at the commission where it will be publicly available.

How do I make a submission?

Submissions can be made in writing or verbally. There is no particular format you need to follow, however, it would assist us if you address the consultation questions listed at the end of the paper.

Submissions can be made by:

- Online form: www.lawreform.vic.gov.au
- Mail: PO Box 4637, GPO Melbourne Vic 3001
- Email: law.reform@lawreform.vic.gov.au
- Fax: (03) 8619 8600
- Phone: (03) 8619 8619, 1300 666 557 (TTY) or 1300 666 555 (freecall)
- Face-to-face: please contact us to make an appointment with one of our researchers.

What happens once I make a submission?

Shortly after you make your submission you will receive a letter or email confirming it has been received. You are then asked to confirm your details by replying within seven days.

Assistance in making a submission

If you require an interpreter, need assistance to have your views heard or would like a copy of this paper in an accessible format please contact the commission.

Confidentiality

When you make a submission you must decide how you want your submission to be treated. Submissions are either public, anonymous or confidential.

- **Public** submissions can be referred to in our reports, uploaded to our website and made available to the public to read in our offices. The names of submitters will be listed in the final report. Addresses and contact details are removed from submissions put on our website.
- **Anonymous** submissions can be referred to in our reports, uploaded to our website and made available to the public to read in our offices but the identity of the author will not be revealed.
- **Confidential** submissions cannot be referred to in our report or made available to the public.

Please let us know your preference along with your submission. If you do not tell us you want your submission treated confidentially we will treat it as public.

More information about the submission process and this reference is available on our website*:* www.lawreform.vic.gov.au

Submission Deadline: 30 June 2009

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 & 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;
- 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.* 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;
- the desirability of building on the work of other law reform bodies.

* Our terms of reference also originally included the publication of photographs without the subject's consent. This issue was removed from the terms of reference by the Attorney-General in October 2006 and referred to the Standing Committee of Attorneys-General (SCAG).

Abbreviations and Acronyms

A Crim R	Australian Criminal Reports
AC	Appeal Cases
ACC	Australian Crime Commission
ALRC	Australian Law Reform Commission
ANPR	Automatic Number Plate Recognition
AFP	Australian Police Force
ASIO	Australian Security and Intelligence Organisation
CCSM	Continuing Consolidation of the Statutes of Manitoba
CCTV	Closed-circuit television
CLEDS	Commissioner for Law Enforcement Data Security
CLR	Commonwealth Law Reports
COAG	Council of Australian Governments
DOJ	Department of Justice
EU	European Union
Eur Court HR	European Court of Human Rights
EWCA Civ	England and Wales Court of Appeal Civil Division
EWHC	England and Wales High Court
FSR	Fleet Street Reports
GPS	Global Positioning System
ICCPR	International Covenant on Civil and Political Rights
ICV	In Car Video
IPA	*Information Privacy Act 2000* (Vic)
IPP	Information Privacy Principle
NICTA	National Information and Communication Technology Australia
NPP	National Privacy Principle
NSWLR	New South Wales Law Reports
NSWLRC	New South Wales Law Reform Commission
NZLC	New Zealand Law Commission
NZLR	New Zealand Law Reports
OCR	Optical Character Recognition
OECD	Organisation for Economic Cooperation and Development
OJL	Official Journal of the European Communities (Legislation)
OPC	Office of the Privacy Commissioner
QB	Queen's Bench
QDC	Queensland District Court
QWN	Queensland Weekly Notes
RFID	Radio Frequency Identification
RSBC	Revised Statutes of British Columbia
RSC	Revised Statutes of Canada
RSNL	Revised Statutes of Newfoundland and Labrador
RSS	Revised Statutes of Saskatchewan
SDA	*Surveillance Devices Act 1999* (Vic)
SMS	Short Message Service
TIA	*Telecommunication (Access and Interception) Act 1979* (Cth)
UDHR	Universal Declaration of Human Rights
VCAT	Victorian Civil and Administrative Tribunal
VCC	Victorian County Court
VLRC	Victorian Law Reform Commission
VSC	Victorian Supreme Court
VSCA	Victorian Supreme Court of Appeal
WLR	Weekly Law Reports

Glossary

Automatic number plate recognition (ANPR)	Technology that recognises symbols in images of a number plate and stores or uses those symbols, for example, to control access to carparks or to identify stolen cars.
Biometric surveillance	Surveillance conducted using biological data, for example, fingerprints, iris patterns or facial features.
Bluetooth	A wireless form of transmission that uses radio waves to transmit information over short distances.
Breach of confidence	When confidential information is disclosed to a wider audience. May result in a right to sue.
Cause of action	A right to sue another person.
CCTV	Closed-circuit television. Now a generic term for surveillance camera systems.
Chilling effect	Where speech or conduct is suppressed because of a belief that it may result in undesirable consequences.
Citizen journalism	Journalism undertaken by non-professionals.
Civil penalty	A fine or other sanction for a civil offence. It has a lower standard of proof than a criminal penalty and there is no finding of criminal responsibility.
Common law	Law that derives its authority from the decisions of courts, rather than from acts of parliament.
Convergence	When used in relation to technology, describes the phenomenon where technology is becoming increasingly interconnected and multi-functional.
CrimTrac	A Commonwealth agency that uses, develops, and provides access to information technology and services for police use.
Data mining	The process of analysing data for known and unknown data patterns.
Data surveillance	The monitoring of data, as opposed to people or places.
Enforcement pyramid	A regulatory model characterised by increasing levels of intervention, utilising serious measures only when milder sanctions (such as education) have failed.
E-tag	A device attached to a vehicle which transmits information to an electronic reader, used to identify the vehicle for tolling purposes.
E-view (Enterprise view)	A web-based tool that provides detailed, zoomable images of buildings and other features compiled through aerial photographs.
Facial recognition	A computer application for identifying or verifying a person from an image, by comparing it with a database of existing images. A form of biometric technology.
Global positioning system (GPS)	A navigation system which relies on information received from a network of satellites to provide the latitude and longitude of an object.

Glossary

Google Earth	A web-based program that maps the earth by the superimposition of images obtained from satellite imagery and aerial photography.
Google Street View	A feature of Google Maps and Google Earth that provides 360 degrees horizontal and 290 degrees vertical panoramic street views and allows users to view parts of some regions of the world at ground level.
Happy slapping	The practice of recording an assault on a victim (commonly with a camera phone) for entertainment.
In car video	A video camera fitted inside a vehicle (for example a police vehicle or taxi). May be used to observe the interior or exterior of the vehicle.
International Covenant on Civil and Political Rights (ICCPR)	A treaty giving effect to civil and political rights contained in the Universal Declaration of Human Rights. Australia is a signatory to the ICCPR.
Location surveillance	Identifying a person's or an object's whereabouts at a particular time.
Mass surveillance	Monitoring the public at large, or a significant part of the public, instead of a particular individual.
Nuisance	An unlawful interference with a person's use or enjoyment of land, or some right over or in connection with it. May result in a right to sue.
Optical character recognition	Software designed to recognise letters and numbers from a captured image and to translate them into editable text.
Optical surveillance	See visual surveillance.
Own-motion investigation	The power of a regulator to investigate possible breaches of a law without the need for a complaint or referral by a person.
Panopticon	A type of prison building designed by Jeremy Bentham to allow for the observation of prisoners without the prisoners being able to tell whether they are actually being watched.
Participant monitoring	Recording of conversations or activities by someone participating in them.
Passive location services	Passive location services are those in which a mobile phone user consents to have his or her location tracked by another person, either from the other person's mobile phone or a computer.
Physical surveillance	Observing a person by being physically present at their location.
Profiling	When used in a law enforcement context, reliance on personal traits (such as race, gender and age) to target potential offenders.
Purpose creep	In a surveillance context, where a surveillance system set up for one purpose is used for another purpose. Also known as 'function creep'.

Radio frequency identification (RFID)	A technology that allows items to be identified through an embedded chip that emits a unique radio signal. There are two forms: active RFID, which emits its own signal, and passive RFID, which is read using energy from an RFID reader.
SmartGate	A project of the Australian Customs and Border Protection Service that uses a biometric passport and face recognition technology to allow eligible travellers arriving at Australia's international airports to self-process through passport control.
Smart card	A card containing integrated circuits that can store and process data. Used for performing financial transactions and accessing restricted areas
Snaparazzi	A play on the word 'paparazzi', used to describe the collection of unstaged and/or candid photographs of celebrities by non-professionals.
Spyware	Software which, once installed in a computer, secretly collects information about the computer use.
Statute	A written law passed by parliament.
Surveillance	Deliberate or purposive observation or monitoring of a person or object.
Tort	A breach of a duty, imposed by law, which protects the bodily integrity, property, reputation or other interests of a person.
Tracking	Monitoring a person or object's whereabouts over a period of time. Also called 'location surveillance'.
Trespass	Direct interference with a person, goods, or property of another without lawful justification. May result in a right to sue.
Universal Declaration of Human Rights (UDHR)	A resolution of the United Nations General Assembly affirming the importance of human rights and listing the rights that UN member countries have pledged to uphold.
Upskirting	The observation or recording of a person's genital or anal region without their consent.
Visual surveillance	Purposeful monitoring of a person or object by sight, including by the use of a device. Also known as 'optical surveillance'.
Voice over Internet Protocol (VoIP)	Generic term for technology allowing delivery of voice communication over the internet and other networks.
Wire-tapping	The use of electronic or mechanical equipment to gain access to transmission of private telephone conversations, computer data or facsimiles.

Executive Summary

SCOPE OF REVIEW

This Consultation Paper introduces the second phase of our inquiry into the use of surveillance and other privacy-invasive technologies. In 2005, we published our *Workplace Privacy: Final Report*.[1] In this paper, we consider surveillance in public places.

Our terms of reference draw attention to the widespread use of surveillance in public places and ask us to investigate whether legislative or other measures are needed to ensure that surveillance practices are appropriately controlled.

OVERVIEW

Surveillance is now part of our everyday lives. We are accustomed to seeing CCTV cameras in shops and at railway stations. Surveillance devices assist with the collection of tolls on freeways, and with stock control and theft prevention when used in product tags in shops. Surveillance technology is used to assist with immigration checks at airports. Many widely owned products now have surveillance capabilities. Mobile phones that are able to take photos, record sound and images and assist us to find our destinations or locate people are common.

Surveillance serves many important purposes including the promotion of public safety and the prevention of crime. It also features in areas such as journalism and entertainment. Many groups within our community use surveillance technology, including police, transport operators, retailers, private investigators, sporting and entertainment venues, and journalists. Despite this widespread use, there is no comprehensive source of information about the extent of public place surveillance in Victoria.

Because of the growing affordability and capacity of surveillance devices we are increasingly likely to be recorded or scrutinised when we are in public places. The ability to store, use and disseminate surveillance data has also grown.

Some of the negative consequences that may flow from the increased use of surveillance in public places include a loss of privacy and anonymity which may cause us to alter the way we express ourselves and behave when in public. While these adjustments may not be readily apparent in the short term, the long-term incremental effect may be permanent changes to the way in which we use and enjoy public places. Because surveillance is often covert, those people with the means to do so may retreat to private places whenever possible in order to avoid unwanted observation.

Because surveillance technology is developing so rapidly, it is time to consider how best to encourage and support its responsible use. The existing regulatory framework has a number of shortcomings which are discussed in the paper.

PRELIMINARY CONSULTATIONS

We have already conducted a number of preliminary consultations with users of surveillance practices and members of the community to better understand surveillance practices in Victorian public places. We also sought views about whether we need to change the law and what form any new regulation should take.

CURRENT PRACTICE

There are a number of surveillance devices that are being used in Victorian public places including CCTV, location and tracking devices, global positioning systems, radio frequency identification, automatic number plate recognition, mobile phones and biometrics. There is also an increasing trend towards the use of mass surveillance to monitor large groups of people. In Chapter 2, we examine these current practices and consider the many factors that are driving the use of surveillance devices. We examine also future trends, looking at possible applications of technological developments.

Both constitutional constraints and practical considerations have limited our inquiries. We have not considered national security uses of surveillance, or telecommunications and data surveillance practices, because these activities are regulated at the federal level. We suggest that surveillance activities conducted by state law enforcement bodies be considered separately because of the need to consider police investigation and information gathering activities as a whole.

PRIVACY

In Chapter 3, we consider the concept of privacy and, in particular, whether it extends to public places. Privacy is an internationally recognised human right which is included in the *Victorian Charter of Human Rights and Responsibilities Act* 2006. It is now widely acknowledged that reasonable expectations of privacy extend to public places. The reasonableness of any expectation of privacy in public will depend on the circumstances, such as whether surveillance is covert, whether a permanent record is created and whether consent has been given.

RISKS AND BENEFITS OF PUBLIC PLACE SURVEILLANCE

Surveillance appears to offer many important benefits to our community including increased safety, crime control, and as a means of expression and journalistic activity. It is appropriate, however, to test the validity of these claimed benefits, especially because the data concerning the beneficial effects of some types of widely used surveillance is limited.

In Chapter 4, we also consider the impact which surveillance in public places can have on privacy and other shared values. Unlike interferences with other important rights, loss of privacy may result in harm which the law finds difficult to characterise and remedy. We consider the impact of the misuse of public place surveillance under the following headings:

- loss of anonymity in public places
- possibility of error and miscarriage of justice
- discriminatory profiling of groups
- voyeuristic uses
- other antisocial uses
- exclusion of groups from public places
- limits to political speech and association
- changes to the nature of public life.

CURRENT LAW

We consider the current regulatory framework in Chapter 5. No single law comprehensively regulates the use of surveillance in public places in Victoria. Three Acts of Parliament regulate some uses of surveillance in public places: the Victorian *Surveillance Devices Act 1999* (Vic) and the *Information Privacy Act 2000* (Vic) and the Commonwealth *Privacy Act 1988* (Cth). Surveillance is also regulated by a range of industry and government codes, self-imposed policies, standards and guidelines.[2] There is no clear public policy that emerges from this body of regulation concerning the circumstances in which public place surveillance is acceptable and the circumstances in which it is not permissible.

The development of laws to cover particularly offensive forms of surveillance, such as 'upskirting' and the recording of images related to child pornography, represent attempts to address some of the limitations in the current regime. In addition, surveillance in some contexts, for example in casinos and bars, is separately regulated.

The existing Victorian regulatory regime is not well equipped to deal with the challenges posed by current and emerging surveillance technology. We identify the types of surveillance practices that may fall beyond existing laws and consider whether the regulatory approaches interstate and overseas offer solutions. We also consider the recommendations of other law reform bodies that are relevant to surveillance in public places. In particular, we have considered the recommendations of the Australian Law Reform Commission (ALRC) concerning information privacy laws.[3] We also examine Australian approaches to regulation in other rapidly changing areas of public concern, such as the environment and the economy.

1 Victorian Law Reform Commission, Workplace Privacy: Final Report (2005).

2 Two tables at the end of Chapter 5 summarise legislation and binding codes and major non-binding instruments relating to public place surveillance in Victoria.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) ch 74.

Executive Summary

REFORM PROPOSALS

The reform options detailed in Chapter 6 are presented for public discussion. That discussion will help us to develop recommendations for inclusion in our final report to the Attorney-General.

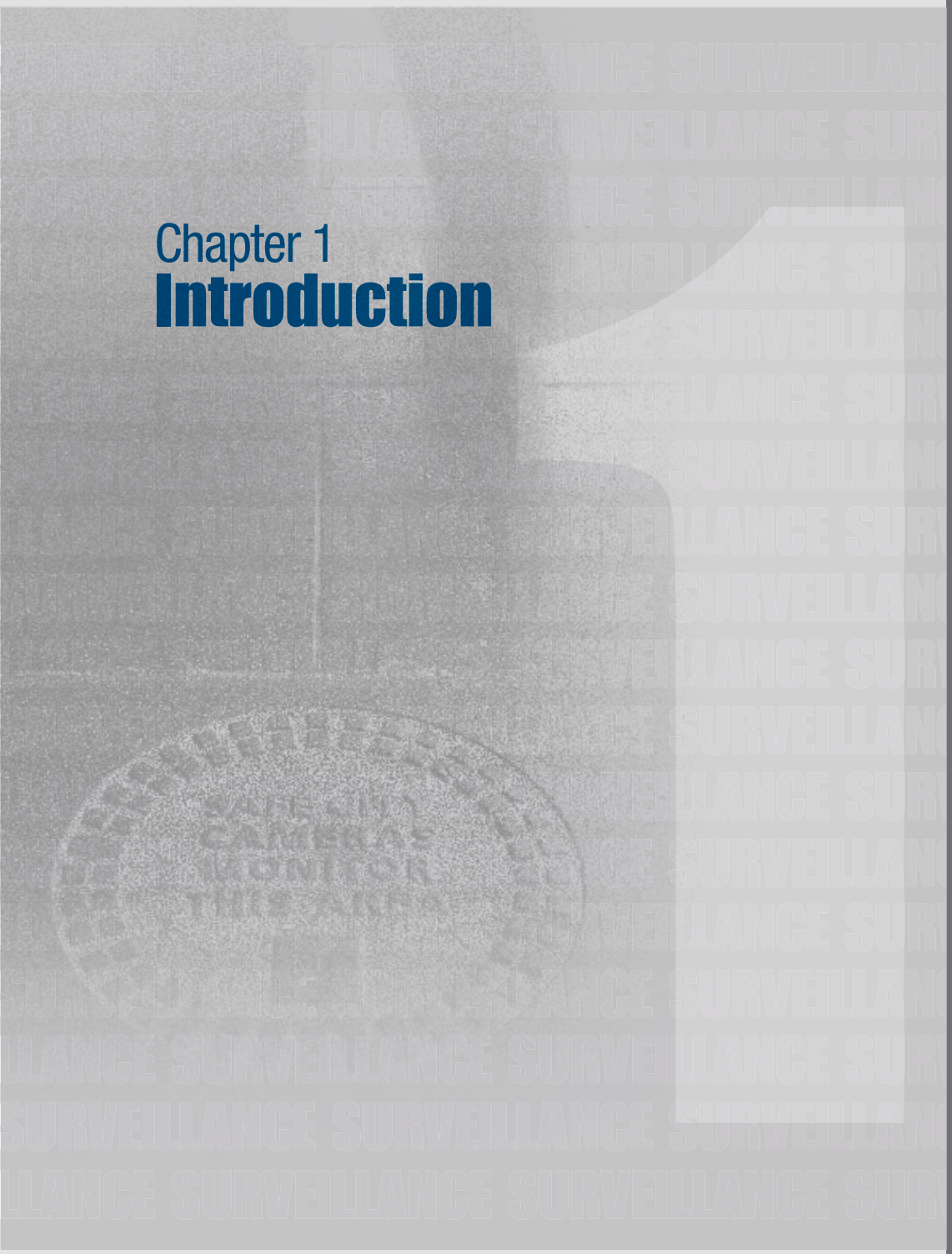
The reform options aim to provide greater certainty and guidance about the situations in which the use of surveillance is acceptable and unacceptable. The commission believes that regulation should be multifaceted and provide sufficient flexibility to address the many contexts in which surveillance occurs and the broad range of people who use surveillance.

We propose a number of overarching principles that may be used to guide regulatory changes and inform policy in Victoria. We ask whether these principles should apply to isolated surveillance practices or should be confined to continuous use of surveillance, for example at a bank or petrol station.

Our reform options include:

- a new role for an independent regulator to monitor, report and provide information about public place surveillance in Victoria. It is envisaged that the regulator may require statutory powers of investigation and could be responsible for regularly reporting to parliament.
- new voluntary best-practice standards to promote responsible use of surveillance in public places. We ask whether compliance with best-practice standards could be encouraged by tying them to Victorian government procurement criteria.
- mandatory codes to govern the use of surveillance in public places with sanctions for non-compliance that include civil or criminal penalties.
- a licensing system for some surveillance practices that are found to be particularly invasive of privacy.
- various changes to clarify and strengthen the *Surveillance Devices Act 1999* (Vic).
- a new statutory obligation to refrain from committing a serious invasion of privacy modelled on the statutory cause of action proposed by the ALRC in its recent report.

Some or all of these options could form part of a new regulatory regime for surveillance in public places in Victoria. The commission has not reached any final views about reform. We encourage submissions on all of the issues and questions raised in this Consultation Paper.



Chapter 1
Introduction

Chapter 1 Introduction

PURPOSE OF THIS CONSULTATION PAPER

1.1 The Victorian Attorney-General asked the commission to inquire into two major issues of public concern in relation to privacy: workplace privacy and the use of surveillance in public places. In October 2005 we published our *Workplace Privacy: Final Report*.[1] That report recommended the government introduce legislation to regulate the testing, monitoring, searching and surveillance of workers in their workplaces.[2] This Consultation Paper introduces the second phase of our inquiry, surveillance in public places.

1.2 Our terms of reference note the widespread use of surveillance in public places. The commission has been asked to consider whether legislative or other measures are needed to ensure that surveillance practices are appropriately controlled now and into the future.[3] In this Consultation Paper we offer a number of options for reform. These options are designed to stimulate public discussion that will assist us when developing reform proposals for inclusion in our final report to the Attorney-General.

1.3 The paper is arranged as follows: Chapter 2 provides an overview of current surveillance practices in Victoria and some likely future trends. It also examines some of the factors driving the use of surveillance devices in public places. Chapter 3 explores the concept of privacy and whether it extends to public places. Chapter 4 considers the risks and benefits associated with public place surveillance. Chapter 5 contains an analysis of the current legal and regulatory framework in Victoria and highlights those surveillance practices that may fall beyond existing laws, as well as considering interstate and international regulatory approaches. Finally, Chapter 6 presents reform options and poses questions for consideration.

BACKGROUND

1.4 Surveillance in public places is not comprehensively regulated in Victoria. Until quite recently, laws of this nature were probably unnecessary. Traditionally, the community took the view that surveillance activities required regulation only when they encroached into the home, or into areas of personal intimacy. However, because of a range of factors, including technological change, the use of surveillance in public places has proliferated. Surveillance devices have become increasingly affordable, available and sophisticated. Some of these devices have the potential to deprive individuals of anonymity and personal space in public because they can monitor movement and capture information in ways that were not previously possible. It is important that we reflect upon this potential loss and consider whether we wish to regulate the use of surveillance in public places.

1.5 Closed-circuit television (CCTV) is the most widely used form of surveillance in both public and private places. It was first used in Australia in Perth in 1991. Since then, its use has increased significantly.[4] Local government authorities, in cooperation with police, now use CCTV systems in the central business districts in most major Australian cities.[5] CCTV is also used to monitor public and private spaces by other organisations including police, transport authorities, retail outlets, and sporting and entertainment venues.[6] The increased use of CCTV is also occurring internationally—the most notable example being the United Kingdom where it was suggested a decade ago that a London resident is likely to be filmed by over 300 cameras on 30 different CCTV systems in the course of a day.[7]

1.6 The capacity to use information gathered by CCTV systems is expanding. There is an increasing tendency for systems to be networked, rather than operating as 'closed-circuit' systems. The majority of modern surveillance cameras now store their footage digitally, allowing images to 'be stored indefinitely, searched, analysed, reproduced and manipulated with increasing ease'.[8] CCTV images can be made available instantly to anyone with the capacity to receive data in this form, and footage may be streamed to the internet or TV.[9]

1.7 Location and tracking devices are now commonly used to determine the whereabouts and movement of individuals in public, as well as private, places. These devices include global positioning systems (GPS) in cars, automatic number plate recognition (ANPR) on tollways, and radio frequency identification (RFID) which is used by businesses to track products (and potentially the individuals who purchased them). A recent example of a controversial surveillance practice is internet search engine Google's launch of Street View in Australia

in August 2008. Street View allows internet users to view photographs of streetscapes and, in some instances, to discover the location of individuals identified in the images.[10]

1.8 Many widely owned products now have surveillance capabilities. An obvious example is the mobile phone (of which there are over 21 million operating in Australia),[11] many of which have the capacity to record sounds and images and to transmit them to multiple destinations, almost instantaneously and at low cost.[12] Mobile phones with GPS capabilities may also be used as tracking devices.[13]

1.9 Public place surveillance has been used for a number of years to fulfil a variety of purposes including public safety, crime detection, investigation and prevention, journalism, recreation, entertainment and marketing.[14] Surveillance is now undertaken routinely in public places by police and other law enforcement officers, business operators, security companies, private investigators, the media, and by individuals. A number of factors appear to be driving the increased use of surveillance in public places, most notably concerns about crime and, more recently, the threat of terrorism. The relatively low costs of surveillance equipment, as well as the increase in its capabilities, may also be contributing to this increase.[15]

1.10 Research has shown some community support for the use of some types of surveillance in public places.[16] However, this support is not absolute. Concerns have been expressed about the potential loss of privacy in public places, the potential misuse of collected information, and the lack of clear evidence supporting the effectiveness of public place surveillance in achieving its stated purposes.[17] A highly publicised United Kingdom example of public opposition to surveillance was MP David Davis's resignation from, and subsequent re-election to, the House of Commons in June 2008. Davis resigned to draw attention to a range of laws and practices that he believed threatened personal freedom, including increased government surveillance.[18] Instances of users of surveillance inappropriately sharing surveillance footage with the media in Victoria have also raised community concerns about the use of surveillance-obtained information.[19]

1.11 While the practice of surveillance in public places continues to grow in Victoria, the use of surveillance devices is not comprehensively regulated. Our existing laws are unclear, they have not kept pace with technological change, and they do not appear to have been actively enforced. It is likely that some organisations and individuals engaging in surveillance practices do not always know whether they are acting lawfully. Further, it appears there is limited community understanding of public place surveillance practices, including what happens to information that has been collected by the use of surveillance.

1 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).

2 In September 2006, the Victorian Parliament enacted the *Surveillance Devices (Workplace Privacy) Act* 2006, which amended the *Surveillance Devices Act 1999* (Vic) to extend its operation into workplaces.

3 Our terms of reference also require us to consider whether any reforms we proposed in our report on workplace privacy in relation to the surveillance of workers could be applied to public places to ensure a consistent approach to regulating surveillance. The terms of reference are reproduced on p7 Our terms of reference previously referred to publications of photographs without the subject's consent. That part of the terms of reference was removed by the Attorney-General in October 2006 as the issue of publication was referred to the Standing Committee of Attorney's-General.

4 John Klepczarek, 'To CCTV or Not To CCTV—That is the Question: But is it the Answer? A Practitioner's Point of View' (Paper presented at the Graffiti and Disorder Conference convened by the Australian Institute of Criminology in conjunction with the Australian Local Government Association, Brisbane, 18–19 August 2003) 2.

5 See Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation: a Report to the Criminology Research Council* (CRC Grant 26/01-02) (2003) 24; and National Community Crime Prevention Programme in partnership with the Australian Institute of Criminology, *CCTV as a Crime Prevention Measure: What is CCTV?* Tip Sheet 5.

6 Use of CCTV in Victoria is further detailed in Chapter 2.

7 Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* (1999) 42.

8 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (2007) 33.

9 Ibid.

10 Andrew Colley, 'Privacy Advocates Say Google's Gone Too Far', *The Australian* (Sydney), 5 August 2008, 3.

11 Australian Communications and Media Authority (ACMA), 'Number of Mobile Phones Now Exceeds Australia's Population' (Press release, 28 April 2008) <www.acma.gov.au/WEB/STANDARD/pc=PC_311135> at 13 November 2008.

12 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info Sheet 05.03 (2003).

13 This is discussed further in Chapter 2.

14 See, eg, Jane Holroyd, 'Police Home in on Noble Park Hoons', *The Age* (Melbourne), 29 January 2007 <www.theage.com.au/news/national/police-home-in-on-noble-park-hoons/2007/01/29/1169919253310.html> at 13 November 2008; Kate Uebergang, 'Name These Hoons', *Herald Sun* (Melbourne), 30 January 2007, 4; Aaron Langmaid, 'Camera Call to Fight Crime', *Caulfield Glen Eira Leader* (Melbourne), 5 November 2007, 7; Mark Buttler, 'Mum Stands up for Rights', *Herald Sun* (Melbourne) 20 December 2007, 22; Kelly Ryan and Ellen Whinnett, 'Strategy to Win back City Streets', *Herald Sun* (Melbourne), 20 December 2007, 2; Ian Royall and Mark Buttler, 'More Cameras Watch City', *Herald Sun* (Melbourne), 26 February 2008, 7; Cameron Houston, 'Violence Prompts Action on Cameras', *The Age* (Melbourne), 27 February 2008, 7; Aaron Langmaid, 'Landlord Locks in CCTV after Gang Bashing', *Port Phillip Leader* (Melbourne), 12 February 2008, 407.

15 Chapter 2 discusses who uses surveillance technology and what is driving that use.

16 This research is perception-based and uses both quantitative and qualitative methods. See Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) i-iii, 50; Wallis Consulting Group Pty Ltd, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner* WG3322 (2007) 3, 74-75; Terry Honess and Elizabeth Charman, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness* (1992) 4-5, 25; Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 1; Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 55, 123; Office of the Privacy Commissioner for Personal Data [Hong Kong SAR], *Community Perceptions Towards Surveillance Cameras in Public Places* (2003) 7, 34.

17 For a discussion on the effectiveness of CCTV, see Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 47-50; see also Wallis Consulting Group Pty Ltd, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner* WG3322 (2007) 74-75.

18 Mr Davis resigned from the Shadow Cabinet and announced his resignation as an MP a day after the narrow passing of a parliamentary vote on British anti-terrorism legislation, which would extend the limit on the period of detention of terror suspects without charge in England and Wales from 28 to 42 days. He stood as the Conservative Party candidate in the subsequent by-election, winning re-election with 72% of the vote, and breaking several voting records in the UK. *Davis Cruises to By-election Win,* (11 July 2008) BBC News <http://news.bbc.co.uk/1/low/uk_politics/7501029.stm> at 13 November 2008.

19 Asher Moses, 'Privacy Fears as Google Hits Road', *The Age* (Melbourne), 10 April 2008, 3; 'Hi-tech Cops Use Cyber Clues', *Community News* (Moonee Valley), 1 April 2008, 16; Kate Uebergang, 'Prison Term Cut for Toilet Spy', *Herald Sun* (Melbourne), 14 November 2007, 2; Mark Dunn, 'Zooming in On Crims: Privacy Worries Over Road Cams Plan', *Herald Sun* (Melbourne), 31 January 2008, 9; and Roundtable 16.

Chapter 1 Introduction

DEFINITIONS

1.12 It is useful to explain what we mean by 'surveillance' and a 'public place'.

WHAT IS SURVEILLANCE?

1.13 The term surveillance comes from the French word 'surveiller', meaning 'to watch over'.[20] The *Macquarie Dictionary* defines surveillance as 'watch kept over a person, etc., especially over a suspect, a prisoner, or the like'.[21] Marcus Wigan and Roger Clarke define surveillance as 'the systematic investigation or monitoring of the actions or communications of one or more persons'.[22] They note four categories of surveillance:

- personal surveillance, which is the investigation or monitoring of an identified person generally for a specific reason
- mass surveillance, which is investigation or monitoring of a large group of people to identify particular members
- object surveillance, which is the investigation or monitoring of an object to detect movement or change in its state
- area surveillance, which is the investigation or monitoring of a physical space, which may or may not include objects or persons.[23]

1.14 David Lyon, a leading writer in the field, defines surveillance as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction'.[24]

1.15 At its broadest, surveillance is any purposeful or routine watching or observation. The purpose of surveillance can be to obtain information[25] or to control behaviour.[26] It may occur in relation to 'everyday human acts' such as 'shopping with loyalty cards, paying for goods with any form of swipe card, visiting a doctor or dentist, using a cell phone, paying utility bills, interfacing with any level of government, [or] logging on to computers using the internet'.[27]

1.16 There are different forms of surveillance. The most common include:

- **Aural surveillance,** which occurs when a person listens to or records a private conversation. Recording may be done overtly or covertly using various forms of voice recorders or 'bugs', such as a small tape recorder or a wire-tap placed on a phone line. Today, aural surveillance devices also include intercepting mobile phone conversations and voice communications over the internet (known as 'voice over internet protocols' or VoIP), such as Skype.
- **Visual surveillance,** which is the purposeful monitoring of a person by sight. It includes the use of a device to visually record or observe a private activity.[28] Examples include CCTV, handheld cameras and cameras in mobile telephones. Images taken and placed on Google Earth and Google Street View are also the result of visual surveillance.
- **Tracking or location surveillance,** which provides information about a person's or an object's whereabouts at a single point in time or over a period of time. An example is GPS, a technology now widely used in cars, mobile phones and personal digital assistants. An estimated 10 to 20 per cent of all mobile phones are GPS enabled.[29] Another widely used tracking technology is RFID, which is used, for example, by businesses to track products in the supply chain.
- **Data surveillance** which is the surveillance of any data and is specifically defined by the *Surveillance Devices Act 1999* (Vic) (SDA(Vic)) as involving the use of a device to monitor or record the input and output of information from a computer.[30] Data surveillance devices include 'spyware' such as keystroke monitoring. Groups that might use data surveillance in Victoria include public libraries monitoring acceptable use of computers,[31] or banking institutions monitoring customer transactions.

- **Biometric surveillance**, which is a new and emerging form of surveillance. It involves the collection of samples of biological information such as fingerprints, face and voice characteristics. This information is then converted into digital form so that it can be stored and compared to later biometric samples in order to identify an individual.[32] Traditionally the police have used this type of surveillance to identify suspects through fingerprint analysis. Modern technology has expanded the use of biometrics. For example, biometric surveillance is now used in Australian and New Zealand passports to track people's movements into and out of the country.[33]

1.17 Surveillance may also involve various forms of personal or human observation that do not require the use of a device. However, we have proceeded on the assumption that human observation must be deliberate or purposive in order to qualify as surveillance. Thus, observations that are a part of everyday activities—such as being observed on the street or on public transport—do not constitute surveillance.

1.18 In summary, the commission believes that surveillance is:

a. deliberate or purposive rather than incidental in nature (this would exclude 'casual observation')
b. either a 'one-off' or systematic practice
c. not exclusively device-dependent (it includes personal observation)
d. used for various purposes.

WHAT IS A PUBLIC PLACE?

1.19 A number of commentators have discussed the difficulties in drawing a clear line between a 'public place' and a 'private place'.[34] An approach based on private ownership of land is not appropriate because so many public activities now take place in premises that are privately owned.[35] In our view, it is more helpful to use a definition that focuses on the degree and nature of accessibility to a place by members of the public. This view is consonant with legislative definitions of 'public place' in a variety of statutory contexts.[36] It is also consistent with views about the definition of public place expressed by various participants during our consultations.[37]

20 *Oxford English Dictionary* (10th ed rev, 2002) 1443.

21 Colin Yallop et al (eds), *Macquarie Dictionary* (4th ed, 2005) 1418.

22 Marcus Wigan and Roger Clarke, 'Social Impacts of Transport Surveillance' (2006) 24 (4) *Prometheus* 389, 391.

23 Ibid 391-392.

24 David Lyon, Surveillance Studies: An Overview (2007) 14. The definition of surveillance used by the Surveillance Studies Network also includes these elements Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [3.1].

25 For example, the New South Wales Law Reform Commission defined surveillance as the use of a surveillance device with the deliberate intention of monitoring a person or place for the purpose of obtaining information. NSW Law Reform Commission, *Surveillance: Final Report* Report 108 (2005) [3.4].

26 The Australian Law Reform Commission defined surveillance as 'the monitoring of a person, place or object to obtain certain information or to alter or control the behaviour of a subject of the surveillance. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [9.89] citing Roger Clarke, *Have We Learnt to Love Big Brother?* (2005) <www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html> at 30 April 2008.

27 Mike Dee, 'The New Citizenship of the Risk and Surveillance Society—From a Citizenship of Hope to a Citizenship of Fear?' (Paper presented at the Social Change in the 21st Century Conference, Queensland, 22 November 2002) 5.

28 This definition does not include devices such as spectacles, contact lenses or devices used by a person with a hearing impairment to overcome that impairment: *Surveillance Devices Act 1999* (Vic) s 3.

29 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

30 This definition draws upon that contained in the *Surveillance Devices Act 1999* (Vic) s 3.

31 For example, libraries may monitor access to inappropriate web sites on library computers, including pornographic sites. Activities of this nature are probably best regulated by the Commonwealth for the reasons outlined later in this chapter.

32 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) 148.

33 *Where are Biometrics Being Used?* Biometrics Institute <www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=133> at 12 November 2008. This is discussed in more detail in Chapter 2.

34 In the context of surveillance, see, eg, Hille Koskela, ''Cam Era'—The Contemporary Urban Panopticon' (2003) 1 (3) *Surveillance & Society* 292; Alison Wakefield, 'The Public Surveillance Functions of Private Security' (2004) 2 (4) *Surveillance & Society* 529. For the purposes of this Consultation Paper, 'place of public resort' and 'public places' are treated as synonymous.

35 For example, while shopping centres, some hospitals and some entertainment venues are privately owned, most people would consider them public places.

36 See *Summary Offences Act 1966* (Vic) s 3; *Fundraising Appeals Act 1998* (Vic) s 3; *Private Security Act 2004* (Vic) s 3; *Casino Control Act 1991* (Vic) s 71; *Child Employment Act 2003* (Vic) s 3; *Classification (Publications, Films & Computer Games) (Enforcement) Act 1995* (Vic) s 3; *Interactive Gambling Act 2001* (Cth) ss 8B and 61AA; *Racial Discrimination Act 1975* (Cth) s 18C(3).

37 For example views expressed in Roundtables 4, 5, 18, 20, 21, 27 and 29.

Chapter 1 Introduction

1.20 The commission believes the broad definition of 'public place' used in the *Racial Discrimination Act 1975* (Cth) is useful:

> public place *includes any place to which the public have access as of right or by invitation, whether express or implied and whether or not a charge is made for admission to the place.*[38]

Places where the public has access 'as of right' include most roads and parks. Places where the public has access by invitation include shops and shopping centres. Places where the public has access upon payment of an admission charge include major sporting arenas and entertainment venues.

1.21 Public places are not necessarily limited to 'physical' spaces. Most forms of technology-based communication (such as radio and telephones) involve communications made by means of electromagnetic waves that are typically carried via electronic pathways. These pathways are essentially public in nature because they are accessible by members of the public and lack the security usually associated with private spaces. It is also possible to describe the online environment of cyberspace as a public space because it is generally accessible to the public.

SCOPE OF THIS PAPER

1.22 Despite our broad definitions of 'public place' and 'surveillance' we have not examined all forms of public place surveillance in Victoria. Constitutional constraints and practical considerations have limited our field of inquiry. For example, we have not considered surveillance that occurs in the workplace because we addressed this in the first phase of this privacy reference.[39] In addition, we do not address the issue of non-consensual publication of photographs because this is the subject of a separate inquiry by the Standing Committee of Attorneys-General.[40]

CONSTITUTIONAL CONSTRAINTS

1.23 Our consideration of some surveillance practices has been limited by constitutional constraints.[41] Section 51 of the Australian Constitution contains a list of matters about which the Commonwealth parliament may make laws, including telecommunications (section 51(v)) and national security (section 51(vi)). The telecommunications power enables the Commonwealth to regulate television, radio, telephones and the internet.[42] The national security power enables the Commonwealth to establish organisations that aim to prevent terrorism. The Victorian parliament may also make laws about the matters set out in section 51. However, where there is any inconsistency between the two, the Commonwealth legislation will override state legislation to the extent of the inconsistency.[43]

Telecommunication and data surveillance

1.24 The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA), regulates the interception of telecommunications and access to communications stored on infrastructure owned by telecommunications carriers. The TIA imposes general prohibitions on these activities, though exceptions exist for authorised interception and access by Commonwealth and state law-enforcement bodies.

1.25 The High Court has decided that the TIA exclusively regulates interception of telephone communications.[44] It is also highly likely that the TIA exclusively regulates interceptions of other communications which take place across telecommunications networks, such as short message service (SMS) and email. Consequently, our consideration of telecommunications surveillance practices is limited. However, it is important to note that the TIA does not provide complete protection against the monitoring of communications across public networks. In particular, it protects telecommunications only while they are passing over the telecommunications system and does not cover interceptions via devices placed next to a phone handset. It also does not apply to communications that do not involve the use of telecommunications equipment, for example, those made solely by radio signals, such as Bluetooth, or walkie-talkie communications.[45] These limitations mean that the Victorian regulation of listening devices, in particular, is important in protecting communications across public networks.

1.26 The existence of the TIA also limits the ability of the Victorian parliament to regulate cyberspace surveillance. Most practices involving the use of computer software to spy on the activities of others via the internet[46] involve telecommunications interceptions. Further, the borderless nature of cyberspace makes it impractical to regulate at a state level. For these reasons, we do not cover cyberspace-related surveillance in this inquiry. However, we do note the importance of appropriate regulation in this area.[47]

1.27 Other data surveillance that is incidental to the activities regulated by the TIA, but does not fall actually within the ambit of the Act, is probably best regulated at the Commonwealth level. An example of such surveillance may be the use of a keystroke monitor to detect use of a computer in an internet cafe or public library.

National security

1.28 We have not examined surveillance practices conducted for national security purposes because this is primarily a Commonwealth responsibility. A number of Commonwealth laws give various bodies including federal and state police, national security organisations and customs specific powers to engage in surveillance activities for security purposes.[48] Recently, these powers have been greatly expanded by a series of laws that form part of a package of anti-terrorism measures.[49] For example, Australian Security Intelligence Organisation (ASIO) officers are permitted to use tracking devices in accordance with a Ministerial warrant 'despite any law of a State or Territory'.[50]

STATE LAW ENFORCEMENT

1.29 The commission has also not examined surveillance activities conducted by state bodies for law enforcement purposes, for example, Victoria Police. The extensive powers possessed by police make it important that there be appropriate limits on their use of surveillance. Police surveillance is generally covert in nature, which increases the potential to intrude into aspects of people's private life, and those of third parties.[51] Also, police are the group most likely to be granted access to privately-owned surveillance systems.[52] In addition, access to government funding means that police can obtain cutting-edge surveillance devices with far greater capacities than are publicly available. Importantly, the consequences of police surveillance can be significant, such as the possible damage to a person's reputation or the potential loss of personal liberty following arrest or conviction.

38 See *Racial Discrimination Act 1975* (Cth) s 18C(3).

39 We have not considered workplace surveillance even where it occurs in a public place (eg, an employer tracking an employee through GPS in the employee's car), as this has been considered in the first phase of our privacy reference. Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [2.8],[3.22]-[3.24].

40 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues* Discussion Paper (2005).

41 Our terms of reference direct us to have regard to 'the interaction between state and Commonwealth laws, and the jurisdictional limits imposed on the Victorian Parliament'. The commission's terms of reference are reproduced on page 7 of this Consultation Paper.

42 For a discussion of the key cases see Geraldine Chin, 'Technological Change and the Australian Constitution' (2000) *Melbourne University Law Review* 25 <www.austlii.edu.au/au/journals/MULR/2000/25.html> at 19 November 2008.

43 *Australian Constitution* s 109. Inconsistencies are not limited to situations where there is an express or direct conflict between federal and state laws; they can also arise where a Commonwealth law is designed or interpreted to be the only law that covers a specific activity.

44 See *Miller v Miller* (1978) 141 CLR 269, 276.

45 See definitions of 'telecommunications network' and 'telecommunications service' in s 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth), which expressly exclude networks and services for carrying communication solely by means of radio communication.

46 For example, the use of viruses or worms like Trojan or rootkit malware infections.

47 For a comprehensive discussion on the international approaches to privacy in cyberspace see Graham Greenleaf, *Global Protection of Privacy in Cyberspace: Implications for the Asia-Pacific* (1998) <austlii.edu.au/itlaw/articles/TaiwanSTLC.html> at 19 November 2008; see the Cyber Law Policy Centre at the University of New South Wales <www.bakercyberlawcentre.org/> at 3 December 2008 .

48 *The Surveillance Devices Act 2004* (Cth) regulates the use of surveillance devices by federal law enforcement officers in relation to Commonwealth-related matters (such as the investigation of Commonwealth offences). That regime complements a similar regime in the *Surveillance Devices Act 1999* (Vic) which regulates law enforcement use of surveillance devices within Victoria. The *Surveillance Devices Act 2004* (Cth) states that it does not affect the operation of State and Territory surveillance laws which means that it is not intended to override any State laws that are able to operate consistently with it. However, the Victorian Act avoids potential inconsistencies by providing for exceptions in respect of activities authorised under Commonwealth law and excludes a number of Commonwealth bodies, including ASIO and the Australian Federal Police.

49 For example the *Anti-Terrorism Act (No. 2) 2005* (Cth) made a number of changes to other legislation, including expansion in the powers of police to question and search persons in relation to terrorist acts and new powers to authorise the use of optical surveillance devices at airports and on board aircraft: see sch 5 and 8. See also Australian Government, *Australian Laws to Combat Terrorism* <www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D49EA90CA256FAB001BA5EA?OpenDocument> at 19 November 2008.

50 *Australian Security Intelligence Organisation Act 1979* (Cth) s 26A.

51 This is because it is undertaken without the consent or knowledge of the subject/s of surveillance and takes place in both public and private places.

52 This is explained in detail in Chapter 2.

Chapter 1 Introduction

1.30 Despite evidence that police surveillance is an important area for further regulation, the commission believes that reform is best achieved through an entirely separate regime from that we propose for general users of surveillance. Principally, this is because surveillance is only one of the many powers of investigation available to police. To consider police use of surveillance in isolation from the broader investigative context would be to consider only part of the picture. Instead, it would be preferable to assess the use of public surveillance for law enforcement purposes in the context of a broader review of all investigative practices.[53] Such a review is beyond the scope of this reference.

1.31 Second, and despite our concerns about proper regulation of police powers of surveillance, police engage in surveillance for a unique and highly compelling reason: preventing and solving crime on behalf of the community. The commission's concern is that many of the options devised for surveillance users generally, such as monitoring by an independent body, may not regulate police practices appropriately.

1.32 Third, police are subject to sanctions for their failure to comply with regulatory requirements that do not apply to other surveillance users in the same way. An example is the inadmissibility of evidence obtained through illegal means, such as unlawful surveillance. While examination of this sanction would be useful when considering the use of surveillance by law enforcement officers, it has little or no relevance to other users of public place surveillance.

1.33 Finally, unlike many other users of public place surveillance, police are subject to numerous other laws (including at the Commonwealth level) that are relevant to their use of surveillance, including laws relating to counter-terrorism investigations. Some of these laws require the sharing of surveillance data with Commonwealth and overseas agencies. Any proposed reform of this area would need to evaluate all of these laws, or again risk assessing only part of the picture.

1.34 It is the commission's view that the cumulative effect of these factors necessitates a separate approach to the regulation of surveillance for law enforcement purposes.[54] This important issue requires separate inquiry by a body that has access to sufficient information about current police surveillance practices in order to devise an appropriate regulatory framework.

THE USE OF INFORMATION OBTAINED THROUGH SURVEILLANCE

1.35 The primary focus of this paper and our reform proposals is on surveillance *practices*—that is, the practices associated with observation and/or recording of a person's behaviour[55]—rather than on the *use* of personal information obtained through such practices. For example, we are primarily concerned with issues such as the appropriateness of the use of CCTV cameras in a particular area, rather than the appropriate use of images captured through CCTV.

1.36 We have taken this approach because the use of information collected by CCTV is likely to be regulated by information privacy laws. Both the Victorian and the Commonwealth parliaments have enacted extensive laws that govern the handling of 'personal information'.[56] These laws contain privacy principles that regulate the collection, storage and use of personal information.

1.37 What happens to information after it is collected through surveillance practices, however, remains important to our review because it is relevant to the protection of privacy and the other important rights and values identified in Chapter 3. For example, the harm caused to a person's privacy by the publication of information collected through surveillance will often be easier to identify and describe than the harm associated with the surveillance practice itself. By way of illustration, people may not take issue with the very widespread practice of filming for personal use on city streets, but once they find their photograph published in a magazine or newspaper, perhaps accompanied by an unfavourable story, they may be greatly concerned about their privacy.[57] More effective control of surveillance practices may prevent subsequent misuse of personal information.

1.38 The Australian Law Reform Commission (ALRC) has recently reviewed information privacy laws in its report *For Your Information: Australian Privacy Law and Practice, 2008* (ALRC report).[58] The report includes 295 recommendations, which, if implemented, would result in an overhaul of privacy regulation in Australia. If all of the ALRC recommendations are adopted, one set of federal privacy principles would apply to all federal government agencies and the private sector,[59] and to state and territory government agencies as well through an intergovernmental cooperative scheme.[60]

1.39 By strengthening information privacy laws, the ALRC recommendations should help protect against intrusions of privacy by public place surveillance, at least for those surveillance practices that amount to the collection of personal information. We have developed our options with the ALRC recommendations in mind.[61]

OUR PROCESS

CONSULTATIONS

1.40 The commission has engaged in preliminary consultations. These consultations have helped us to understand how public place surveillance is conducted and regulated in Victoria, as well as the reasons for its use and the way its use affects the community.

1.41 In October 2007, the commission published a brochure *Are you being watched?* on surveillance in public places encouraging the public to submit their thoughts about this topic to the commission.

1.42 In 2006 and 2007 the commission held 31 roundtable discussions with users of surveillance, privacy advocates and community groups. These included representatives from state government organisations, police, local councils, universities and technical and further education (TAFE) institutions, transport operators, businesses (including media organisations, retailers and sports and entertainment venues), courts, security and investigation organisations, Indigenous justice bodies and young people, as well as other community representatives and private citizens.

1.43 These consultations provided a valuable insight into the types of organisations that use surveillance in public places in Victoria as well information on surveillance practices, for example the number of CCTV cameras that are in use. Information about the extent of surveillance is not broadly available, or even collected in Victoria.

1.44 In addition, our discussions with technology experts provided us with information about how surveillance technologies work in practice, and about future trends in surveillance technologies. Finally, our consultations with community-based organisations, individuals and representatives from marginalised groups provided valuable information on the impact of surveillance practices in public places.

RESEARCH

1.45 We have conducted extensive research into the regulation of surveillance in Victoria, other Australian jurisdictions and overseas. We have also considered our research and recommendations in relation to workplace privacy, as well as subsequent legislative developments.[62] In addition we have looked at the writings of a number of leading commentators and the work of a number of other law reform commissions.

1.46 In 2005, the New South Wales Law Reform Commission (NSWLRC) published *Surveillance: Final Report* which proposed a broad legislative approach to regulating both covert and overt forms of surveillance[63] in private and public places. More recently, the NSWLRC has released a consultation paper (*Privacy Legislation in NSW)* which examined the adequacy of NSW personal information and health information legislation,[64] with a view to providing an effective framework for the protection of individuals' privacy. [65] While this consultation paper touches on the use of surveillance devices, this is not its specific focus.

53 For example, the New Zealand Law Commission published a report in 2007 dealing with the search and surveillance powers of all law enforcement agencies. New Zealand Law Commission, *Search and Surveillance Powers* Report 97 (2007).

54 The recent leaking of confidential files from the Victoria Police's covert surveillance unit to organised crime figures highlights the complexity of issues that surround police surveillance. The incident lends support to commission's view that consideration of police surveillance practices would be best undertaken by a body that has broad ranging access to covert police units as well as police information and policies. See Nick McKenzie and Richard Baker, 'Secret Police Files Leaked', *The Age* (Melbourne) 2 December 2008, 1.

55 A person's behaviour can include actions, movements, conversations and other forms of communication.

56 *Privacy Act 1988* (Cth); *Information Privacy Act 2000* (Vic). The Acts define personal information as recorded information or an opinion about an individual, whether true or not, whose identity is apparent, or can reasonably be ascertained, from the information or opinion: *Privacy Act 1988* (Cth) s 3; *Information Privacy Act 2000* (Vic) s 3.

57 See eg, Yan Mei Ning, 'Media Photography in Hong Kong Streets: The Impact of Proposed Privacy Torts' (2006) 11 (2) *Media and Arts Law Review* 161, 168 discussing the case of woman who complained to the Privacy Commissioner about a photograph of her taken without her knowledge or consent and published to illustrate an article about fashion sense.

58 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008).

59 Ibid 10 (Recommendation 18-2).

60 Ibid 112, 219 (Recommendation 3- 4).

61 We note that our terms of reference refer to 'the desirability of building on the work of other law reform bodies'. The commission's terms of reference are reproduced on page 7 of this Consultation Paper.

62 Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002), Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004), Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).

63 NSW Law Reform Commission, *Surveillance: Final Report,* Report 108 (2005).

64 NSW Law Reform Commission, *Privacy Legislation in NSW, Consultation Paper 3* (2008), considering in particular the *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2002* (NSW); *Health Records and Information Privacy Act 2002* (NSW); *State Records Act 1998* (NSW); *Freedom of Information Act 1989* (NSW); and the *Local Government Act 1993* (NSW).

65 See Ibid viii.

Chapter 1 Introduction

1.47 The New Zealand Law Commission (NZLC) is also undertaking a Privacy Review and in 2008 published a study paper *Privacy: Concepts and Issues* to provide a 'policy overview of privacy values, changes in technology and international trends' and their implications for New Zealand.[66] The NZLC will shortly publish an issues paper for stage 3 of the review, which will examine civil law remedies for invasion of privacy, as well as the adequacy of the criminal law for invasions of privacy.

1.48 In 2004, the Law Reform Commission of Hong Kong published two key reports related to privacy and surveillance: *Civil Liability for Invasion of Privacy*[67] and *Privacy and Media Intrusion*.[68] In 1998, the Law Reform Commission of Ireland published a report entitled *Privacy: Surveillance and the Interception of Communications*.[69]

1.49 We have referred to the findings of these law reform commissions wherever they deal with issues we consider.

NEXT STEPS

1.50 Information about how to give us your views is set out on page 6. To allow time for the commission to consider your views before deciding on recommendations, please provide your submission by 30 June 2009.

1.51 The commission will also engage in targeted consultations with surveillance users and organisations with an interest in privacy issues. The aim of these consultations will be to seek responses to the various reform proposals included in this paper and to obtain further information about the nature of public place surveillance practices in Victoria.

1.52 After completing our consultations and reviewing submissions, the commission will provide the Attorney-General with a final report containing recommendations for reform. We aim to complete this reference by the end of 2009.

66 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [1.4].

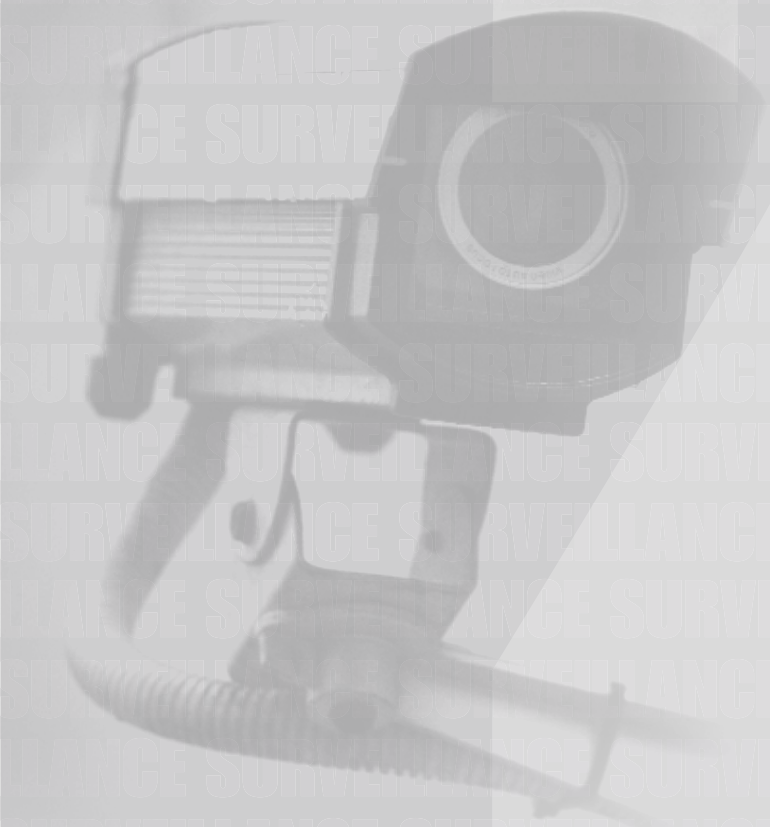
67 Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* Report (2004).

68 Law Reform Commission of Hong Kong, *Privacy and Media Intrusion* Report (2004).

69 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998).

Chapter 2

Current Practice



Chapter 2 Current Practice

INTRODUCTION

2.1 This chapter examines the various forms of public place surveillance in Victoria, who uses it, and why. We provide an overview of recent trends in public place surveillance and examine key technologies. We also examine the factors that may be driving the increased use of public place surveillance and consider future trends.

2.2 Public place surveillance has become widespread in Victoria and its use is increasing. Victorians can expect to be observed, recorded and tracked while engaged in daily activities in our streets, shops and at major public venues. In addition, surveillance technologies are more sophisticated and have greater capacity to store, use and disseminate data.

2.3 There is no single comprehensive source of information about the extent of public place surveillance in Victoria. Therefore, our overview of this issue has been informed by the results of our preliminary discussions with major users of public place surveillance and our examination of research that has been published. Further discussions with major users of public place surveillance will take place prior to the publication of our final report.

BACKGROUND

2.4 In Chapter 1, we describe public place surveillance as any form of purposeful monitoring of an individual or individuals, with or without a technological device, that occurs in a public area. We defined public area to include any area where the public has access as of right (for example, roads and parks) or by invitation (for example, stores and shopping centres).

2.5 While surveillance in one form or another has always been with us, some recent trends are worth noting:

- the use of increasingly sophisticated technological devices with greater capacities
- the declining cost of surveillance devices and their greater use by businesses and individuals
- increase in mass surveillance which monitors large groups of people rather than specific individuals
- the widespread use of location and tracking devices
- the increased capacity to store, use and disseminate surveillance data.

All five trends are apparent in Victoria and are discussed in more detail below.

TRENDS IN PUBLIC PLACE SURVEILLANCE

INCREASING SOPHISTICATION OF SURVEILLANCE DEVICES

2.6 Modern public place surveillance makes use of some very sophisticated devices and advances in technology have occurred at a rapid pace. For example, prior to the late 19th century it was seldom possible to take a person's photograph without their knowledge.[1]

2.7 Advances in technology subsequently enabled covert photography. Thus, from 1938 to 1941 noted New York photographer Walker Evans was able to take his covert shots of passengers on the New York City subway, in violation of a ban on subway photography.[2]

2.8 Surveillance devices, such as beepers or pagers (electronic transmitting devices that trace location) and video cameras have been in use in some countries for decades.[3] For example, a 1957 study of local and state government surveillance in the United States found tracking devices and hidden cameras were widely used by police, prosecutor's offices and a host of other government entities.[4]

2.9 Recently, more sophisticated technologies have become widely available. Police around the world increasingly have a range of surveillance devices at their disposal including 'see-through' technology (capable of seeing through walls and clothing),[5] facial recognition technology (where cameras scan people gathered in a public place matching faces to database of wanted criminals),[6] and satellite photography.[7]

2.10 Other examples of sophisticated surveillance technologies include:

- devices that contain powerful, compact and concealable cameras which can now be placed in everyday objects
- closed-circuit television (CCTV) systems that use digital technology and can be networked, some having the capacity to zoom, pan and tilt and to record audio and visual information.
- mobile phones that are able to record and send audio and visual information as well as track movements and find locations.
- radio frequency identification (RFID) technology that is incorporated in product tags to prevent theft, improve stock control and process sales more quickly, used in car-key fobs to open and identify cars and on freeways to collect road tolls.
- optical character recognition (OCR) technology that enables information in scanned photographs to be read and compared with data for identification purposes—for example, reading a number plate to identify the owner of a car.

2.11 The Commonwealth government has made significant investments in surveillance technologies. For example, the 2004–05 Commonwealth Budget allocated $17.2 million over four years to 'modernise and expand the surveillance capabilities of Australian Government agencies'.[8] The media reported last year that the Australian Crime Commission intends to build a broad ranging 'bugging' system, capable of intercepting electronic communications, including video and photographs sent from mobile phones, conversations in internet chat rooms, telephone calls made using the internet, and communications made through various wireless networks.[9]

2.12 While there is a trend towards the use of surveillance devices with greater capacities, it is important to note that personal surveillance, or human observation, has not ceased. The commission was told in consultations that personal surveillance is one of the most common forms of covert surveillance used by police.[10] Personal surveillance is also commonly used by the transport sector,[11] at businesses[12] and sporting venues,[13] and by private investigators.[14]

1 Aimee Jodoi Lum, 'Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Sphere' (2005) 27 *Hawaii Law Review* 377, 377 citing Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 (5) Harvard Law Review 194, 211.

2 Aimee Jodoi Lum, 'Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Sphere' (2005) 27 *Hawaii Law Review* 377, 377.

3 Christopher Slobogin, 'Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards' (1997) 10 (3) *Harvard Journal of Law & Technology* 383, 386 citing Alan F Westin, *Privacy and Freedom* (1967) 173.

4 Ibid 386, citing Alan F Westin, *Privacy and Freedom* (1967) 173.

5 Ibid 386 citing Fox Butterfield, 'New Devices May Let Police Spot People on the Street Hiding Guns', *New York Times* (New York), 7 April 1997, A1, A10.

6 Such software was reportedly used in 2001 by the Tampa Police Department in the state of Florida in the United States, in a downtown nightlife district: Andrew Taslitz, 'The Fourth amendment in the Twenty-first Century: Technology, Privacy, and Human Emotions' (2002) 65 *Law and Contemporary Problems* 125, 125 citing Dana Canedy, 'Tampa Scans the Faces of Its Crowds for Criminals', *New York Times* (New York) 4 July 2001, A1, A11.

7 Christopher Slobogin, 'Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards' (1997) 10 (3) *Harvard Journal of Law & Technology* 383, 386, citing Fox Butterfield, 'New Devices May Let Police Spot People on the Street Hiding Guns', *New York Times* (New York), 7 April 1997, A1, A10. In Victoria, police have access to night vision technology (Roundtable 5). Another example of the use of sophisticated surveillance technology in policing is the use of infrared cameras by the NSW police to gain intelligence about illegal oyster farming. New South Wales Food Authority, *'Joint Operation to Tackle Illegal Oyster Scam'* (Press Release, 4 April 2007) <www.foodauthority.nsw.gov.au/aboutus/media%2Dreleases/mr%2D04%2D04%2D07%2Doperation%2Dtrident/> at 10 November 2008

8 Commonwealth Attorney-General, *Investing in Australia's Security* <www.budget.gov.au/2004-05/bp2/html/expense-02.htm> at 10 November 2008.

9 Julian Bajkowski, 'Crime Fighter to Build Bugging System', *The Australian Financial Review* (Sydney), 5 October 2007 <www.misaustralia.com/viewer.aspx?EDP://20071005000019505067> at 10 November 2008.

10 Roundtable 5.

11 The transport industry uses approximately 550 ticket inspectors for observational surveillance of customers on trams and trains in Victoria: roundtables 19, 23.

12 For example, a supermarket reported using personal observers in its stores: roundtable 14; and a department store reported using uniformed loss-prevention personnel to deter theft: roundtable 15.

13 Roundtable 4.

14 Roundtable 25.

Chapter 2 Current Practice

DECREASING COST AND GREATER AVAILABILITY

2.13 Use of sophisticated surveillance technologies is no longer exclusive to the military, government agencies and other specialists. Due to lower costs and increasing availability businesses and private citizens also have access to this technology.[15] Many surveillance devices are now available at low cost at electronics stores, hardware stores and office supply stores as well as over the internet.

2.14 Some of the devices available include those capable of being 'hidden in teddy bears, VCRs, smoke alarms, lamps, light bulbs, wall clocks, air purifiers and radios'.[16] One advertised product is capable of zooming in on small and distant objects, allowing 'license plates to be clearly identified from a distance of 160m'.[17] Cameras the size of a five cent piece are now widely affordable.[18]

2.15 Private investigators also make use of camera surveillance.[19] The commission learned from consultations that advances in technology (making cameras that are more compact and readily concealable) have greatly increased the ability of investigators to monitor a subject.[20] Cameras as small as pens can now be placed in one room while the activities monitored are watched from a room next door.[21]

2.16 Many mobile phones are potential surveillance devices which are becoming increasingly cheaper to own. There are over 21 million mobile phones operating in Australia.[22] Many phones record sounds and images and transmit them almost instantaneously to unlimited destinations at low cost.[23] Mobile phones can also act as tracking devices through built-in global positioning technology.[24] An estimated 10 to 20 per cent of all mobile phones have this capability, and it is suggested this figure could increase to 30 to 40 per cent by the end of this decade.[25]

MASS VISUAL SURVEILLANCE

2.17 Another recent phenomenon is the rise of 'mass visual surveillance'.[26] Mass surveillance, in contrast to targeted forms of surveillance, monitors the public at large, rather than specific individuals.

2.18 While mass visual surveillance can evoke George Orwell's novel *Nineteen Eighty-Four*[27] with its 'telescreens' monitoring the public for a totalitarian state, mass surveillance (usually in the form of CCTV) is now the norm in many communities where it is used by local councils, shopping centres, public transport operators and small businesses. Other modern forms of mass visual surveillance include speed cameras, traffic flow cameras,[28] satellite images and x-ray body scanners being trialled in some Australian[29] airports that penetrate clothing to reveal items that may be hidden by passengers on their body.[30]

Closed-circuit television

2.19 CCTV was made possible by the advent of videotape and the video cassette recorder (VCR) which allowed images from a camera to be replayed instantly.[31] In 1967, Photoscan launched CCTV in the retail sector for the purpose of deterring and apprehending shoplifters.[32] It was not until the 1990s, however, that the use of CCTV became widespread.[33]

2.20 A CCTV system is one in which a number of video cameras are connected through a closed circuit or loop, and images are sent to a television monitor or recorder.[34] The term closed circuit highlights the private nature of the system and distinguishes it from television broadcasting where anyone can receive signals.[35] Modern CCTV cameras use digital technology and are no longer 'closed circuit' but 'are networked digital cameras with expanding capabilities'.[36] The expression CCTV is still commonly used, however, to refer to camera surveillance.[37]

2.21 Many CCTV cameras are able to full pan, tilt and zoom[38]—that is, they are not always fixed in one position. Some also have night vision, motion detection and automatic tracking capabilities.[39] Technological developments have led to the inclusion of microphones in some cameras enabling users to 'eavesdrop on the conversations of people as they are filmed'.[40] The United Kingdom has recently introduced 'talking CCTV cameras' that allow council

staff to talk to pedestrians to tell them, for example, to place their rubbish in bins.[41] Some CCTV systems are also used in conjunction with other technologies, for example facial recognition software, allowing cameras to identify faces in a crowd that match faces on a database.[42] 'Smart surveillance systems' are being developed that link behaviour analysis technology with CCTV. These systems use 'automatic image understanding and allow surveillance officers to observe a wide area quickly and efficiently, and to alert them to 'suspicious' behaviour.[43]

CCTV in Australia

2.22 The first Australian CCTV system was installed in Perth in 1991. Since then the use of CCTV has become widespread.[44] Most central business districts now have them[45] and a survey of Australian local councils in 2005 found that around nine per cent owned or directly operated CCTV systems.[46] The Victorian figure was slightly lower.[47]

2.23 There is little information available about the number of CCTV cameras in use in Victoria.[48] There is no central register that records the location and ownership of surveillance cameras in public places.[49] We have used the limited published information and that obtained through our preliminary consultations to build a picture of the nature and extent of CCTV use in Victoria.

2.24 Melbourne City Council's open-street CCTV system (the 'Safe City Cameras Program') has 23 cameras in various locations in the central business district,[50] with an additional 29 scheduled to be installed.[51] *The Sunday Age* reported in 2007 that there were 3000 surveillance cameras in Melbourne petrol stations, 2500 in pubs and clubs, 2000 in the Chadstone Shopping Centre, 2000 in post offices, milk bars and newsagents and 1200 in chemists.[52]

15 For example Short Courses Victoria is offering courses on 'Installation of Video Surveillance Equipment (Digital Video Recorders)', 'Installation of Video Surveillance Equipment (IP Security Cameras)' and 'Installation of Video Surveillance Equipment (Pan Tilt Zoom Cameras)' see <www.shortcourses.vic.gov.au/> at 10 November 2008.

16 See Mark Russell, 'The Spying Game: Privacy Threatened by Rise in Hidden Cameras' *The Age* (Melbourne), 30 September 2007, 7.

17 See *AXIS 233D Network Dome Camera 35X Zoom Progressive Scan 360,* Provantage <www.provantage.com/axis-0266-001~7AXIC0AR.htm> at 10 November 2008.

18 They can be purchased for as little as $70: See Mark Dunn and Jacqueline Freegard, 'Perverts' Snapshots Hit the Net', *Herald Sun* (Melbourne), 24 January 2007, 21.

19 Roundtable 25.

20 Roundtable 25.

21 Roundtable 25.

22 Australian Communications and Media Authority (ACMA), 'Number of Mobile Phones Now Exceeds Australia's Population' (Press release, 28 April 2008) <www.acma.gov.au/WEB/STANDARD/pc=PC_311135> at 13 November 2008.

23 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info Sheet 05.03 (2003).

24 Global Postitioning Technology is discussed in detail later in this chapter.

25 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

26 Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: the Rise of CCTV* (1999) 19.

27 George Orwell, *Nineteen Eighty-Four* (first published 1949, 2000 ed) 55.

28 Mike Dee, 'The New Citizenship of the Risk and Surveillance Society—From a Citizenship of Hope to a Citizenship of Fear?' (Paper presented at the Social Change in the 21st Century Conference, Centre for Social Change Research, Queensland University of Technology, 22 November 2002).

29 Melbourne, Sydney and Adelaide.

30 Lisa Martin, 'Stripping for Air Safety', *The Age* (Melbourne), 27 October 2008, Education Section 12.

31 Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: the Rise of CCTV* (1999) 18.

32 Ibid.

33 Ibid.

34 Benjamin Goold, *CCTV and Policing* (2004) 12.

35 Ibid 12.

36 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008)140 citing Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (2007) 33.

37 Department of Justice, Victoria, *CCTV Toolkit for Victoria: Is CCTV the Best Response?* (2007) 3. We note that this document is no longer available on the Department of Justice website.

38 Privacy International, *CCTV: Frequently Asked Questions* (1997) <www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61925> at 10 November 2008; Benjamin Goold, *CCTV and Policing* (2004) 18. 'Full pan and tilt' refers to the ability to control the camera remotely allowing the controller to move or tilt the camera in order to view from a variety of angles.

39 Ibid.

40 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (2007) 33.

41 Martin Wainwright, 'Talking CCTV Cameras Accuse the Wrong Person', *Guardian* (London), 12 April 2007 <www.guardian.co.uk/uk/2007/apr/12/ukcrime.humanrights> at 10 November 2008.

42 Nick Huber, 'If the Face Fits, You're Nicked' *The Independent*, 1 April 2002 <www.independent.co.uk/news/business/analysis-and-features/if-the-face-fits-youre-nicked-656092.html> at 10 November 2008.

43 Suyu Kong, 'Classifying and Tracking Multiple Persons for Proactive Surveillance of Mass Transport Systems' (Paper presented at The University of Queensland Information Technology and Electrical Engineering Seminar, University of Queensland, 27 June 2007) <www.itee.uq.edu.au/events/seminars/archive/2007/sem-0034.html> at 18 December 2008; Arun Hampapur et al, *The IBM Smart Surveillance System* <www.research.ibm.com/peoplevision/CVPR04SSEDemo.pdf> at 18 December 2008.

44 National Community Crime Prevention Programme in partnership with the Australian Institute of Criminology, *CCTV as a Crime Prevention Measure: What is CCTV?* Tip Sheet 5

45 See Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* A Report to the Criminology Research Council (CRC Grant 26/01-02) (2003) 24; and National Community Crime Prevention Programme in partnership with the Australian Institute of Criminology, *CCTV as a Crime Prevention Measure: What is CCTV?* Tip Sheet 5

46 IRIS Research, *Australian Council's CCTV Survey 2005* Final Report (2005) 8.

47 Ibid 9. Adam Sutton and Dean Wilson, 'Open-Street CCTV in Australia: The Politics of Resistance and Expansion' (2004) 2 (2/3) *Surveillance & Society* 310

48 For a limited survey of public place surveillance use in Australia, see Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006).

49 Although there have been calls for such a register: Mark Russell, 'Smile for the Cameras: There May be One Watching You Now' *Sunday Age* (Melbourne), 26 June 2007, 8.

50 City of Melbourne, *Safe City Cameras* <www.melbourne.vic.gov.au/info.cfm?top=183&pg=1299> at 2 October 2008; and Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* A Report to the Criminology Research Council (CRC Grant 26/01-02) (2003) 36 [4.4.3].

51 Cameron Houston, 'Violence Prompts Action on Cameras', *The Age* (Melbourne), 27 February 2008, 7.

52 Mark Russell, 'Smile for the Cameras: There May be One Watching You Now' *Sunday Age* (Melbourne), 26 June 2007, 8.

Chapter 2 Current Practice

A Victoria Police initiative launched in November 2008 uses a CCTV van fitted with five surveillance cameras on its roof to patrol popular nightspots in Melbourne to deter and identify offenders associated with alcohol related violence.[53]

2.25 The commission's consultations in 2007 with various users of public place surveillance in Victoria supplements this limited published information. In consultations it was suggested that roughly a third of all public buses are fitted with surveillance cameras,[54] as are nearly all trams[55] and taxis.[56] Train stations in Victoria typically have between 1 and 10 cameras (although a few have up to 150).[57] There are also more than 400 CCTV cameras monitoring traffic on Victoria's roads[58] and 180 cameras stationed around Melbourne's port.[59] This is comparable to findings published in 2001 for the New South Wales transport sector, where there were 5,500 cameras at rail stations, and extensive use of CCTV on buses, ferry wharves and many taxis.[60]

2.26 CCTV use by retailers,[61] and sporting and entertainment venues[62] is also widespread. Most shopping centres do not monitor their CCTV live, but record and store images for different lengths of time.[63] Our consultations revealed that live monitoring occurs more often where there is a mass gathering of people, such as at sporting events and inner city train stations.[64] For example, one sport and entertainment venue uses 140–150 cameras that operate 24 hours a day and are constantly monitored by security staff.[65]

2.27 The commission also consulted local councils. Some of the CCTV systems used by councils are quite sophisticated. For example, one council reported that its surveillance system is motion-activated and that once triggered it can send images to the palm-pilots of designated police officers, technicians and council employees.[66] Another council reported that its system, also motion-activated, is linked to a database of pre-recorded graffiti 'tags' or signatures.[67]

2.28 Council systems are sometimes operated in conjunction with other groups, including police, local traders and government agencies.[68] For example, one council's cameras are linked directly to the local police station. Police can override council control of the system, redirecting cameras in particular directions.[69] More generally, councils allow for varying degrees of police access that range from providing footage to police on request to providing direct or 'live' vision of footage from surveillance cameras to police stations.[70]

2.29 It also appears that councils monitor CCTV systems differently. For example, one council does not monitor at all due to the expense involved and another suggested its system is monitored 24 hours a day, seven days a week.[71]

2.30 The commission also consulted with Victoria Police about their use of CCTV. Police use of CCTV involves accessing footage from surveillance cameras owned and operated by others, including local councils, transport operators and private businesses. As noted above, police access to council systems can be direct. In addition, police have direct access to at least one transport body's surveillance cameras[72] and can request that those cameras be moved.[73]

2.31 Another example of law enforcement use of CCTV is the Crime Stoppers program. This program places surveillance footage, some of which is from CCTV, on a website to elicit information from the public about an alleged crime.[74] Members of the public can also upload images captured on their mobile telephones onto the Crime Stoppers web site.[75]

2.32 Victoria Police have also recently introduced in car video (ICV). ICV involves fitting police cars with both front and rear cameras so that the driver can see what is happening inside and outside the car.[76]

2.33 Private individuals also use CCTV for area surveillance of their premises. CCTV systems for home use cost only a few hundred dollars.[77] While these cameras are used primarily to monitor and record activities within people's homes and gardens, they may have a public place dimension if they view activities beyond the perimeter of the monitored property. The Victorian Privacy Commissioner has received enquiries about surveillance cameras that incidentally or intentionally capture activities or views of adjacent properties.[78]

Google Earth and Google Street View

2.34 Internet search engine Google has developed and made widely accessible two forms of mass visual surveillance: Google Earth and Google Street View. Google Earth puts satellite and aerial photographs of the earth onto a three dimensional world map that can be searched. The resolution of the images using Google Earth differs between cities, but in most cases buildings can be identified while number plate numbers cannot.[79] The photographs are reportedly taken at intervals of a year or more.[80]

2.35 Google Street View allows a user to navigate a city at street level through a series of photos forming a 360-degree panoramic view. Google gathers the images using vehicles that drive along public streets.[81] The project currently covers streets in major cities in Australia, the US, France, Italy and Japan.[82] Street View images have much higher resolution than those of Google Earth.

2.36 While the images on Google Earth and Google Street View are not viewed in real time, and internet users cannot control the cameras, the applications can be used for surveillance purposes. In Victoria, recent media reports examined councils' use of Google and other mapping programs. At least one report suggests that local councils are using the Google Earth technology to identify illegal building activity including unauthorised renovations and demolitions, breaches of heritage regulations and unregistered animals.[83]

2.37 It has also been reported that the Sydney City Council is using a tool called E-View to zoom in on detailed aerial photographs of residents' addresses. The resolution of the photographs allows council staff to 'see anything bigger than 10 centimetres by ten centimetres'.[84] For example, there were recent reports in the media about a NSW council's refusal to grant a resident a street-parking permit after it determined by using satellite imagery that the person had parking space in his backyard.[85]

53 See Kellie Cameron, 'Police Surveillance Van Captures Quiet Melbourne Crowd', *Herald Sun* (Melbourne), 15 November 2008 <www.news.com.au/heraldsun/story/0,21985,24655419-661,00.html> at 9 January 2009; and Victoria Police, 'Police Tackle Public Order Offences Head on' (Press Release, 10 November 2008) <www.police.vic.gov.au/content.asp?Document_ID=17806> at 9 January 2009.

54 Roundtable 19.

55 Roundtable 19.

56 Roundtable 10. A trial of externally placed still and video cameras is reportedly underway on trams to reduce pedestrian accidents and improve driver behaviour. If implemented, it could eventuate in fines and demerit points for motorists speeding past stationary trams. Stephen Moynihan, 'Snap! Tram-Stop Sneaks Will Be in the Picture', *The Age* (Melbourne), 2 July 2007, 1.

57 Roundtable 23 and statistics provided by the Department of Infrastructure to the Victorian Law Reform Commission on the basis of surveys conducted at train stations by the Department of Infrastructure in February and March 2008.

58 Roundtable 3.

59 Roundtable 10.

60 National Community Crime Prevention Programme in partnership with the Australian Institute of Criminology, *CCTV as a Crime Prevention Measure: What is CCTV?* Tip Sheet 5 , 3 citing ARTD (2001).

61 Roundtables 14 and 15.

62 Roundtable 4.

63 Roundtable 31.

64 Roundtable 4.

65 Roundtable 13.

66 Roundtable 6.

67 Roundtable 6.

68 Roundtable 6.

69 Roundtable 7.

70 Roundtable 7.

71 Roundtable 7.

72 Roundtable 3.

73 Roundtable 3.

74 Crime Stoppers, *Sharing Crime Information Online* <www.vic.crimestoppers.com.au/articleZone.aspx?articleZoneID=11> at 11 November 2008.

75 Ibid.

76 Victoria Police, 'First In Car Video Vehicles Launched' (Press Release, 25 July 2007) <www.police.vic.gov.au/content.asp?Document_ID=11796> at 11 November 2008.

77 For example, on a quick search for 'security and surveillance' on www.amazon.com we found pages of surveillance cameras and equipment starting at US$125.

78 Email from Office of the Victorian Privacy Commissioner to the Victorian Law Reform Commission, 4 December 2008.

79 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

80 Ibid

81 Google, *Where Does Street View Imagery Come From*? <maps.google.com/support/bin/answer.py?answer=70191&topic=11640> at 11 November 2008.

82 See Google Street View, <maps.google.com.au/maps?layer=c&z=4&utm_campaign=en_AU&utm_medium=ha&utm_source=en_AU-ha-apac-au-gns-svn&utm_term=main_button> at 11 November 2008.

83 Cameron Houston, 'I Spy with My Google Eye', *The Age* (Melbourne), 24 September 2008, 3.

84 Sunanda Creagh, 'They Know Where You Live: Big Council is Watching You', *The Sydney Morning Herald* (Sydney), 18 September 2008, 1.

85 Ibid.

Chapter 2 Current Practice

2.38 Other potential surveillance applications of Google Street View include its use by potential stalkers and burglars to 'scope' houses,[86] and the proliferation of web sites containing embarrassing or voyeuristic shots from Google Street View (for example, images of women sunbathing).[87]

WIDESPREAD USE OF LOCATION AND TRACKING DEVICES

2.39 Another recent trend is the increased use of location and tracking devices for surveillance purposes. A location device gives information about a person or an item's whereabouts at a single point in time. A tracking device gives information about a person's or an item's location over time.[88] Developed by the military and once used primarily by police,[89] tracking devices are now embedded in many widely used products, such as mobile phones.

Global Positioning Systems

2.40 Many location devices rely on a technology called global positioning system (GPS).[90] GPS is now found in many cars and in handheld objects, such as mobile phones and personal digital assistants.[91] GPS also has many practical applications, including navigation and map-making.[92]

2.41 In Victoria, taxi drivers are using GPS to assist them to find drop off and pick up points, and to determine travel routes. In an incident reported in the media in 2007 police used a taxi's GPS system to track and locate a woman who had stolen the taxi.[93] Trams are also tracked using GPS,[94] and the City of Melbourne has asked for comment on the use of GPS as part of a traffic congestion-charging program for the city.[95]

2.42 GPS is also being used in innovative ways by businesses to gather information apart form location. For example, it has been reported that an Australian marketing company has given people who deliver catalogues a GPS device to collect information about households, such as whether fences need painting and which neighbourhoods have children and pets, when they deliver catalogues. It has been suggested that this marketing information would then be on-sold to other businesses and advertisers.[96] An Australian car-sharing program is using GPS in its vehicles that display advertising to report to its advertisers where members have driven, and thus, where the car's advertising is likely to have been seen.[97]

2.43 In the United States, car hire companies use tracking devices to monitor the speed of their customers and adjust their charges accordingly. In one case in Connecticut, a company charged clients a penalty when they exceeded the speed limit for more than two minutes at a time.[98]

Radio Frequency Identification

2.44 RFID is another type of tracking device. RFID allows identification of a specific object, place or person without having them in direct line-of-sight.[99] The technology relies on small tags known as 'transponders' (or RF tags) that transmit and receive radio signals to and from scanners (the RF reader).[100]

2.45 RFID has been in use for some time. In World War II the British used this technology to determine whether incoming aircraft were 'friend or foe'.[101] Today, RFID is serving non-military uses. According to the RFID Association Australia:

> *You probably already use RFID technology everyday. For example, keyless entry systems on cars use a small RFID reader (a key fob) and an RFID tag (inside your car). When these two match, entry to your vehicle is granted.*[102]

2.46 There are two types of RFID tags: active and passive. An active RFID tag is powered by an internal source, such as a battery, and is constantly functioning. According to the CASPIAN advocacy group, '[m]ost tags being considered for use in consumer products are passive.'[103]

2.47 A passive RFID tag is powered by an external source, such as an e-tag reader on a Melbourne freeways. Mechanisms have been installed along freeways to enliven and read the e-tags in passing vehicles. This allows the e-tag to communicate the identity of the vehicle to the reading device in order to charge a toll for freeway use. A passive RFID tag cannot be used to monitor the location of a vehicle constantly, but it will identify that vehicle when it is near a reader.

2.48 Retailers also use RFID technology. Clothing and other items are tagged and read by readers at shop exits to prevent theft.[104] Other stores use RFID for more rapid goods checkout.[105] The 'key driver' of RFID for businesses, however, is its use to track products within the supply chain,[106] ensuring, for example, that retailers' shelves remain stocked.[107] Importantly, unlike barcodes, RFID tags can be read even when they are within boxes or behind walls.[108] It has been suggested that RFID could replace barcodes on products within the next 10 years.[109]

2.49 RFID technology is also being used for surveillance of individuals. For example, RFID tags are used in home detention schemes. In Victoria, those eligible for the scheme are required to wear a bracelet with an RFID tag installed. The tag is linked to a telephone landline and also to a unit monitored by a supervising officer, who is able to determine the location of the wearer at all times.[110] In addition, at least one prison operator in Australia plans to fit prisoners and staff with wrist or ankle tags containing RFID tags to monitor their movements within the prison.[111] In 2008, the UK government proposed to fit dementia patients with wristbands containing RFID tags to allow aged care centres to track patients at home, although the suggestion has received some criticism.[112]

2.50 In the United States, the Food and Drug Administration has approved the use of RFID tags as small as rice grains for insertion in the arms of patients. It is proposed that these tags will contain medical information, which health care providers can access should a patient be unable to communicate his or her medical history.[113] It has been suggested that this may be useful for Alzheimer's patients if they arrive alone at a hospital.[114]

86 David Vaile, 'Google Street View' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

87 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008). See *Google Street View Sightings,* <www.gstreetsightings.com/> at 13 November 2008. This website contains videos of images captured by Google Street View, the images are categorised by the website into any one of the following classifications: ' funny', 'trouble', 'interesting', 'weird', 'girls', 'film & TV' and 'my heroes'.

88 Roger Clarke, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

89 Christopher Slobogin, 'Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards' (1997) 10 (3) *Harvard Journal of Law & Technology* 383, 386, citing Fox Butterfield, 'New Devices May Let Police Spot People on the Street Hiding Guns', *New York Times* (New York), 7 April 1997, A10.

90 'GPS' means global positioning system, which refers to a group of satellites that constantly orbit the earth emitting radio signals: Frederick Lane, *The Naked Employee: How Technology is Compromising Workplace Privacy* (2003) 199. Signals are sent to a network of satellites that enable the holder of a GPS device, for example a person or car, to calculate its position on the earth.

91 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

92 Global Positioning System, *Serving the World* <www.gps.gov/> at 11 November 2008.

93 'Taxi chase ends after 90kms', *The Age* (Melbourne), 13 December 2007 <www.theage.com.au/articles/2007/12/13/1197135588830.html> at 11 November 2008.

94 Roundtable 19; See also, *Tram Tracker,* Yarra Trams <www.yarratrams.com.au/desktopdefault.aspx/tabid-80/121_read-766/> at 14 January 2009.

95 See City of Melbourne, *City Of Melbourne Invites Public Comment on Future Melbourne Draft Plan* (16 May 2008) <www.melbourne.vic.gov.au/info.cfm?top=228&pg=715&st=967> at 17 June 2008. This states that the proposed outcomes of the draft *Future Melbourne* plan include 'a GPS network-based automated congestion charging system to operate in the municipality'.

96 Simon Lauder, 'Junk Mail Deliverers to "Spy" on Households', *ABC News Online*, 23 May 2006 <www.abc.net.au/news/stories/2006/05/23/1645382.htm> at 11 November 2008.

97 *Car Advertising Benefits with Smartpilots Australia,* Smartpilots: Mobile Advertising and Communications <www.smartdrivers.com.au/sd/benefits.aspx> at 9 January 2009.

98 This was ruled an illegal contractual penalty by the Connecticut Supreme Court: Anita Ramasastry, *Tracking Every Move you Make: Can Car Rental Companies Use Technology to Monitor Our Driving?* (23 August 2005) <writ.news.findlaw.com/ramasastry/20050823.html> at 23 October 2008.

99 RFID Association of Australia, *What is RFID?* <www.rfidaa.org/what-is-RFID> at 11 November 2008.

100 Privacy Commissioner [New Zealand], 'Tracking Technology on the Move' (2005) 54 *Private Word* 1, 1; Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 3 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

101 Privacy Commissioner [New Zealand], 'Tracking Technology on the Move' (2005) 54 *Private Word* 1, 1.

102 RFID Association of Australia, *What is RFID?* <www.rfidaa.org/what-is-RFID> at 11 November 2008.

103 Consumers Against Supermarket Privacy Invasion and Numbering, *RFID: Nineteen Eighty-Four* <www.spychips.com/faqs.html> at 11 November 2008.

104 RFID Association of Australia, *What is RFID?* <www.rfidaa.org/what-is-RFID> at 11 November 2008.

105 Ibid.

106 Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 3 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

107 Australian Retail Industry Guidelines, *RFID in Retail: Consumer Privacy Code of Practice* [draft] (January 2007) 4 <www.gs1au.org/assets/documents/products/epcglobal/epc_privacy_review.pdf> at 11 November 2008.

108 Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 6 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

109 Privacy Commissioner [New Zealand], 'Tracking Technology on the Move' (2005) 54 *Private Word* 1, 1.

110 Department of Justice [Victoria], *Home Detentions Questions and Answers* (2005) 6.

111 ACT Corrective Services has announced its intention to use RFID to track prisoners and staff, and has contracted to roll out the technology in the Alexander Maconochie centre. This technology has also been introduced in parts of Europe including Sweden and the Netherlands as well as the United States: Marcus Browne, *ACT Prison to RFID Tag Inmates* (18 April 2008) ZDnet Australia <www.zdnet.com.au/news/security/soa/ACT-prison-to-RFID-tag-inmates/0,130061744,339288184,00.htm> at 11 November 2008.

112 Stephanie Kennedy, 'Controversy over Dementia Tracking Tags' <www.abc.net.au/news/stories/2008/01/02/2130380.htm> at 11 November 2008.

113 Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 8 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

114 Medical News Today, *AP Report on RFID Chips and Cancer Raises Concerns* (10 September 2007) <www.medicalnewstoday.com/articles/82032.php> at 11 November 2008.

Chapter 2 Current Practice

2.51 RFID chipping is currently the preferred method for permanently identifying dogs and cats[115] and in Victoria it is usually a prerequisite for pet registration.[116] Other examples of overseas applications of RFID technology include use in university identification cards in the US and China that enable students to register their attendance at lectures and conduct library applications without a librarian.[117] The Exploratorium museum in San Francisco provides visitors with RFID-enabled cards to use in museum exhibits. The cards activate cameras which provide a personalised record of the museum experience for inclusion on a webpage.[118]

Automatic Number Plate Recognition

2.52 Another technology that can be used for location and tracking surveillance is automatic number plate recognition (ANPR). ANPR uses both a camera and OCR software to take an image of a car, locate the car's number plate within that image and convert the number plate to text.[119] The car's number plate can be matched to a car registration database[120] to identify the car owner or other matters of interest.

2.53 ANPR can be used automatically to send out speeding fines and to charge vehicle owners for their use of toll roads.[121] ANPR can also be used to compare vehicles to lists, such as lists of stolen cars.[122] ANPR has already been put to both uses in Victoria. CityLink, a network of toll roads in Melbourne, relies on ANPR to charge users of toll roads. If a car driver does not pay the mandatory toll, CityLink uses ANPR to identify the owner of the car in order to take recovery action. [123]

2.54 In 2006 four Melbourne petrol stations participated in a trial of ANPR to identify the owners of cars involved in the theft of petrol. Cars were photographed as they entered a petrol station and checked against a list of cars involved in petrol theft. Cars that appeared on the database in the cross match were then prevented from filling up. The data that was collected was shared with police. It has been reported that this data is being retained indefinitely.[124]

2.55 A shopping centre in Victoria is testing ANPR in car parks to track the entry and exit times of vehicles and length of visits so that it can better manage its car park.[125] The program is of interest to police, as they can be notified when a stolen car has entered the car park.[126]

2.56 CrimTrac, a Commonwealth agency,[127] is currently investigating the development of a national ANPR system in Australia to help police detect criminal activity where it involves the use of motor vehicles.[128] It is suggested that the technology would allow police to 'track the movement of cars across the country and pull over criminals or drivers of stolen vehicles.'[129] It is currently preparing a report outlining options and the feasibility of such a system.[130]

Mobile phones

2.57 As we noted earlier, mobile phones are increasingly able to act as surveillance devices. Because mobile phones regularly communicate their location to a base station to make or receive calls, they 'effectively identify the location of the user every few minutes'.[131] In addition, an estimated 10 to 20 per cent of all mobile phones have GPS.[132] The GPS systems in mobile telephones could potentially assist in locating a person in an emergency.[133] In the United States, the technology has allowed parents to track their children's movements via mobile phones held by their children.[134] According to Andrew McNamee, while parental tracking is not as widely accepted in Australia, its usage is growing.[135]

2.58 Several shopping centres in the UK are using a special technology that is able to track customers' mobile telephones while the customer is in the centre.[136] The technology detects a mobile phone's signal and measures its distance from three receivers located within the centre. According to a media report, the centre is thereby able to obtain useful marketing information for example, that 'a majority of customers who visited Gap also went to Next' or that 'an unusually high percentage of visitors were German.'[137]

Biometrics

2.59 Biometrics involves the collection of samples of biological information, such as fingerprints and face or voice characteristics, for later comparison with samples provided by the same person, or different individuals, to establish identity.[138] Biometrics can operate as a form of location and tracking surveillance because they can be used to determine if a person was at a particular location at a certain time. For example, a school in New South Wales has reportedly begun fingerprinting students to track school attendance and borrowing of library books.[139]

2.60 In Australia and New Zealand, biometrics are used in passports to register people's movements into and out of the country. Travel documents known as ePassports now contain embedded microchips which store the passport holder's 'digitised photograph, name, gender, date of birth, nationality, passport number and the passport expiry date'.[140] The SmartGate program, in Brisbane, Cairns, and Melbourne International Airports, uses information in the ePassport and face recognition technology together 'to perform the customs and immigration checks that are usually conducted by a Customs officer'.[141] Facial recognition technology has been introduced with the aim of improving 'identity verification' and reducing identity fraud.[142] Similarly, some overseas airports are using iris recognition technology with frequent flyers.[143]

2.61 The use of facial recognition technology in conjunction with CCTV has been employed in the US to search for individuals. At the 2001 Super Bowl, for example, 100,000 fans were filmed covertly and their faces compared with those in police databases.[144] Similarly, in Las Vegas, casinos use facial recognition technology to identify known 'gambling cheats',[145] and in some airports it has been applied to control 'access to restricted areas by comparing surveillance images to known terrorists'.[146]

2.62 Facial recognition technology is not widely used by the Victorian organisations we consulted. The commission was told that the technology has not advanced sufficiently for retail use[147] and is not cost effective.[148] Nevertheless, one venue is beginning to use it at entry points to identify 'serial pests'.[149] More commonly, businesses rely on regular photography to find serial offenders. One retailer stated that it distributes photos of recidivist offenders to their loss-prevention officers and in some cases police.[150] Another venue distributes photographs of past offenders, downloaded from its CCTV system, to its security guards on the ground.[151]

115 *2001 RSPCA Australia Scientific Seminar,* RSPCA <www.rspca.org.au/events/seminar2001.asp> at 9 December 2008.

116 *Domestic (Feral and Nuisance) Animals Act 1994* (Vic) s10C(a). Note that pursuant to s 10D(3) 'A Council may resolve that class of dog or cat is exempted from any requirement to be implanted with a prescribed permanent identification device for the purposes of registration'.

117 Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 18 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

118 Sherry Hsi and Holly Fait, 'RFID Enhancing Visitors' Museum Experience at the Exploratorium' (2005) 48(9) *Communications of the ACM* 60; and Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *RFID: Frequency, Standards, Adoption and Innovation* (2006) 18-19 <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008.

119 Crimtrac, *Automated Number Plate Recognition* <www.crimtrac.gov.au/systems_projects/AutomatedNumberPlateRecognitionANPR.html> at 11 November 2008.

120 Roger Clarke, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

121 Marcus Wigan and Roger Clarke, 'Social Impacts of Transport Surveillance' (2006) 24 (4) *Prometheus* 389, 396.

122 Ibid 396.

123 Roger Clarke, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

124 Clay Lucas, 'Spycam for Petrol Thieves Fuels Rights Debate', *The Sunday Age* (Melbourne), 30 July 2006, 2.

125 Roundtable 31.

126 Roundtable 31.

127 Crimtrac was established as an Executive Agency in the Attorney-General's portfolio under the *Public Service Act 1999* (Cth). Its specific role is proscribed by an Inter-Governmental Agreement signed by all Australian police ministers: *About Us* (2008) CrimTrac <www.crimtrac.gov.au/about_us/index.html> at 18 November 2008.

128 Crimtrac, *Automated Number Plate Recognition* <www.crimtrac.gov.au/systems_projects/AutomatedNumberPlateRecognitionANPR.html> at 11 November 2008.

129 Jonathan Pearlman, 'Police Track Numberplates Nationally', *Sydney Morning Herald* (Sydney), 20 September 2007, 2.

130 Crimtrac, *Automated Number Plate Recognition* <www.crimtrac.gov.au/systems_projects/AutomatedNumberPlateRecognitionANPR.html> at 11 November 2008.

131 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) 145.

132 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

133 ibid.

134 Andrew McNamee, 'Ethical Issues Arising From the Real Time Tracking and Monitoring of People Using GPS-based Location Services' (2005) 35-36 <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1003&context=thesesinfo> at 9 January 2008. See, eg, 'Tracking teens: Parents use GPS Cell Phones to Keep up with Their Children' LA Times/Washington Post wire service, 27 June 2006, <medialab.semissourian.com/story/1158246.html> at 30 June 2008.

135 Andrew McNamee, 'Ethical Issues Arising From the Real Time Tracking and Monitoring of People Using GPS-based Location Services' (2005) 36 <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1003&context=thesesinfo> at 9 January 2008.

136 Jonathan Richards, *Shops Track Customers Via Mobile Phone* (16 May 2008) Times Online <http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece> at 12 November 2008.

137 Ibid.

138 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) 148.

139 Daniel Emerson, 'Fingerprinting Schoolkids Gets My Vote: Iemma', *Sydney Morning* Herald (Sydney), 3 April 2008 <www.smh.com.au/news/national/fingerprinting-schoolkids-gets-my-vote-iemma/2008/04/03/1206851075570.html?sssdmh=dm16.309282> at 12 November 2008 and *Where are Biometrics Being Used?* Biometrics Institute <www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=133> at 12 November 2008.

140 *Where are Biometrics Being Used?* Biometrics Institute <www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=133> at 12 November 2008.

141 Australian Customs Service, *Smartgate* (2008) <www.customs.gov.au/site/page.cfm?u=5552> at 12 November 2008.

142 Department of Foreign Affairs and Trade [Australia], *The Australian ePassport* <www.dfat.gov.au/dept/passports/> at 12 November 2008.

143 At Schiphol Airport in the Netherlands for example, those who choose to utilise the iris scan enjoy expedited border control procedures and priority parking. See: Amsterdam Airport Schiphol, *Privium* <www.schiphol.nl/web/show/id=67508/langid=42> at 13 November 2008.

144 Marcus Nieto et al, *Public and Private Applications of Video Surveillance and Biometric Technologies* (2002) 6.

145 Ibid 7.

146 Ibid 7.

147 Roundtable 15.

148 Roundtable 31. One participant said the technology was unreliable as it can be rendered useless by someone wearing a cap: Roundtable 14.

149 Roundtable 4.

150 Roundtable 15.

151 Roundtable 15.

Chapter 2 Current Practice

Other location and tracking devices

2.63 Other examples of location and tracking surveillance technologies include the Myki public transport ticketing system which the Victorian Government proposes to implement in the next few years.[152] That system will provide passengers with smart travel cards that can calculate and automatically deduct fares from pre-paid accounts.[153] Except when issued on an anonymous basis, these cards have the potential to track and record a person's movements throughout the transport system.[154] Such system are in use in the United Kingdom with the 'Oyster' card and in Hong Kong with the 'Octopus' card.

2.64 Further, it was reported that in November 2007, five Geelong nightclubs installed an electronic system to record patrons' details upon entry, and to check those details against a list of patrons who had been barred from attending any of the clubs for drunkenness or violence. The data collected by the nightclubs includes the patron's name, address, date of birth, driver licence number and photograph, which is deleted within 28 days unless the patron has been barred from one of the clubs.[155]

INCREASED CAPACITY TO STORE, USE AND DISSEMINATE DATA

2.65 A final trend to note is the increasing ease with which information gathered by surveillance devices can be stored, searched and disseminated. This is in large part due to the move from analogue to digital technology. As the Royal Academy of Engineering has explained, digital technology has permitted two significant developments:

> *First, digital recording capacities mean that images can be stored indefinitely, searched digitally, analysed, reproduced and manipulated with increasing ease. Second, images from any camera can be made available instantly to anyone with the capacity to receive data in this form.*[156]

In addition, the internet now allows databases containing information captured by surveillance to be stored online then accessed and searched remotely.[157]

2.66 According to David Lyon, modern surveillance systems 'increasingly depend on searchable databases'.[158] For example, surveillance data can be 'mined' and 'matched' to other sources of data such as facial recognition software that compares an image on CCTV footage to a database of faces of interest.

FACTORS DRIVING THE USE OF SURVEILLANCE TECHNOLOGY

2.67 The uses and users of surveillance have changed markedly over the past few years. Surveillance technology is now more widely available than ever and it is able to collect and disseminate information in ways previously not thought possible. What explains the increased use of surveillance technologies by government, businesses and individuals? What purposes does public place surveillance serve in Victoria? In the next part of the chapter we take a closer look at who uses public place surveillance in Victoria and why.

CRIME CONTROL

2.68 Victoria Police told the commission that surveillance is an important part of criminal investigations[159] and a key factor in obtaining convictions in areas such as organised crime.[160] Other reasons underlying police use of surveillance include:

- obtaining evidence of criminal activity[161]
- enhancing the ability to investigate corruption offences and other forms of crime that are covert, sophisticated and difficult to detect by conventional methods[162]
- encouraging more defendants to plead guilty to charges because of surveillance evidence[163]
- reducing the potential for harm to police, undercover operatives and informants, because they can be forewarned of planned reprisals and criminal activities.[164]

2.69 Retailers seeking to reduce theft is another key reason for the use of surveillance. CCTV and RFID technology are widely used in the retail sector for the purpose of deterring and apprehending shoplifters.[165] In our consultations, a retailer suggested that theft causes losses of approximately $3 billion annually.[166] In addition, newsagents reportedly find that 4.5 per cent of their turnover is 'walking out the door'.[167] Petrol stations have reported that up to $5 million is lost in 'drive off' thefts each year.[168]

2.70 A number of businesses told us that surveillance technology, most notably CCTV, has helped reduce theft. For example, the placement of overt CCTV cameras in petrol stations has reportedly reduced the number of hold-ups and drive offs.[169] In addition, we were informed that CCTV can help in the prosecution of theft after it has occurred by allowing businesses to share images with police, although business groups noted that the images must be of high quality to be useful.[170] Museums told the commission that a lending gallery's insurer often requires surveillance systems for international exhibitions.[171]

2.71 Transport operators and local councils also use surveillance for crime-prevention purposes. They suggested that cameras might serve as a general deterrent to crime and other antisocial behaviour on trains, trams and buses.[172] Local councils told the commission they used surveillance cameras in the hope that they will prevent a range of behaviour including assault, vandalism, drug dealing, street-car racing, drunk and disorderly behaviour and sale of tobacco to underage children.[173] Cameras are also installed in skateboarding and graffiti areas to protect property.[174]

2.72 Businesses were also concerned about the impact of crime on the personal safety of employees and customers. One retailer reported that surveillance was an important tool to protect its workforce.[175] Employee safety is a particular concern for businesses that are vulnerable to armed hold ups, such as petrol stations and bottle shops.[176]

2.73 Some community groups acknowledged the crime control benefits of public place surveillance.[177] For example, the commission was told that homeless people may derive a sense of safety from the presence of cameras.[178] At the indigenous justice roundtable, the value of surveillance to public safety was also noted and the failure of surveillance systems to capture incidents of assault was identified as a problem.[179]

2.74 Counter-terrorism measures are also likely to have contributed to the increased use of public place surveillance. The impact of the events of September 11, 2001 in the United States and the terrorist attacks in Bali, Madrid and London has

152 See *Melbourne's Myki Two Years Late* (25 March 2007) MIS Online <www.misaustralia.com/viewer.aspx?EDP://1206415258258> at 12 November 2008.

153 *How Will I Use Myki?*, Myki <www.myki.com.au/use-myki_your-key.aspx> at 12 November 2008.

154 See discussion in Peter Ker, 'Have Card, Will Travel', *The Age* (Melbourne), 15 July 2007, 11.

155 Mark Buttler, 'Clubs Test ID System' *Herald Sun* (Melbourne), 15 November 2007, 18; Ellen Whinnett and Mark Buttler, 'No Licence, No Drink: Push to Log Patrons in Pubs, Clubs', *Herald Sun* (Melbourne), 16 October 2007, 9.

156 Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (2007) 33.

157 David Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) 19 (2) *International Sociology* 135 139.

158 Ibid 142.

159 In 2004, Victorian courts issued 150 surveillance device warrants for the investigation of state crimes, Court warrants are only one measure of the frequency of surveillance device use since law enforcement officers do not need to obtain a warrant in all circumstances—see Chapter 5. Most of these warrants were issued to Victoria Police. Other warrants for surveillance and interception of communications were issued to the Australian Crime Commission (10), the Victorian Department of Primary Industries (8) and the Victorian Department of Sustainability and Environment (4): Victorian Parliament Law Reform Committee, Warrant Powers and Procedures, Final Report (2005) 371 <www.parliament.vic.gov.au/lawreform/> at 14 May 2008.

160 Roundtable 5.

161 Roundtable 5.

162 Roundtable 30.

163 Roundtable 16.

164 New South Wales, Royal Commission into the New South Wales Police Service, *Final Report* (1997) vol 2, 413.

165 Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: the Rise of CCTV* (1999) 18.

166 Roundtable 15.

167 Roundtable 20.

168 Clay Lucas, 'Spycam Trap for Petrol Thieves Fuels Rights Debate', *The Sunday Age* (Melbourne), 30 July 2006, 2.

169 Roundtable 15.

170 Roundtable 20.

171 Roundtable 4.

172 Roundtables 3, 4.

173 Roundtables 6, 7 and 8.

174 Roundtable 6.

175 Roundtable 15.

176 Roundtable 15.

177 Roundtable 22.

178 Roundtable 16.

179 Roundtable 28.

Chapter 2 Current Practice

been significant. Lyon has written that the events and consequences of September 11 'are catalyzing surveillance developments in several countries simultaneously.'[180] In Australia, concerns about terrorism have resulted in the passage of a number of anti-terrorism laws, including laws which permit surveillance.[181]

2.75 Australian federal and state governments have promoted the development of a 'surveillance infrastructure' by encouraging local government and business to install or upgrade surveillance systems to assist in counter-terrorism efforts,[182] and by directly providing funding for surveillance systems in some instances.[183] The Council of Australian Governments' (COAG) *National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism*[184] aims to enhance the capacity of CCTV in Australian mass passenger transport systems to assist with counter-terrorism. The federal government's 'National Security Hotline'[185] asks individuals to observe or monitor members of the community in order to alert authorities to possible terrorist activities.

2.76 During consultations, some businesses cited counter-terrorism as a reason for their use of surveillance technology[186] and discussed federal and state governments' efforts to encourage private sector use of CCTV.[187] For example, retail groups referred to COAG's interest in information from their surveillance activities[188] and efforts to have them upgrade the image quality of their surveillance cameras.[189]

2.77 In consultations we were also told that businesses share surveillance data with counter-terrorism agencies. For example, during the World Economic Forum held in Melbourne in September 2000 cameras were installed on the upper floors of one business's building which were subsequently used by police.[190] An advocacy group for shopping centres reported that it meets with the security industry and large building managers quarterly on anti-terrorism issues[191] and noted the creation of the business–police partnership against terrorism (Mass Gatherings Infrastructure Advisory Assurance Group).[192]

2.78 While crime prevention and control is a major reason for using CCTV, the evidence suggests that its effectiveness in reducing crime is open to debate. We examine the effectiveness of CCTV in Chapter 4.

RESPONDING TO ACCIDENTS AND MANAGING CROWDS

2.79 Surveillance cameras are also used to ensure public spaces remain accident free by monitoring crowd behaviour. Large stores and entertainment venues use surveillance for public safety purposes[193] and for crowd control.[194] Cameras are monitored and information is passed on to ground staff about how best to manage crowd movement.[195]

2.80 Public safety is an important reason underlying transport sector use of surveillance. For example, surveillance cameras can assist transport operators to respond when a fire has erupted[196] and cameras on trams allow the driver to know when an elderly passenger has sat down.[197] There are also over 400 CCTV cameras operated by road authorities for the purposes of traffic monitoring and accident response.[198] Safety is also a major reason for surveillance use by local councils,[199] where surveillance allows for monitoring volumes of road traffic, access for emergency vehicles and crowd flow.[200]

2.81 Dealing with potential liability for injuries to shoppers through 'slip and fall claims' is another reason why shopping centres use CCTV.[201] If CCTV captures an incident on video it was suggested that the business is better placed to respond to a potential claim. Using surveillance technologies can also reduce the premium for insuring against these claims.[202] One business group stated that the first thing a public liability insurer will ask is whether you have CCTV.[203]

OTHER OPERATIONAL NEEDS OF BUSINESSES

2.82 In some situations, CCTV is a cheaper means of securing premises or stock than traditional security measures such as foot patrols by security guards. In consultations, a shopping centre operator reported that the days of having large numbers of security staff have passed because of financial constraints[204] and that CCTV is becoming the main surveillance tool in many industries.[205]

2.83 Public place surveillance is also used in a number of other ways to replace people. For example, one council told us that it had installed cameras at entry and exit points in its gym as a means of reducing the number of personnel required.[206] Surveillance devices are also used in the transport sector to see if service targets are being met. [207]

FRAUD AND OTHER INVESTIGATIONS

2.84 Surveillance in public places is also an investigative tool. In this context it is usually covert. For example, private investigators aim to be discreet, and they will discontinue surveillance or change the mode of surveillance if the subject is aware of being monitored.[208] Private investigators commonly use surveillance to investigate insurance claims.[209] For example, insurers use private investigators to conduct surveillance of people who have made claims against the government,[210] and surveillance footage is a very important source of evidence in insurance litigation.[211]

JOURNALISM

2.85 Public place surveillance is a tool used by journalists who photograph, film and record people's activities in public places when they report on news and current affairs. The commission consulted with broadcast news outlets, print journalists and photographers' organisations about their use of surveillance. [212]

2.86 Media surveillance usually occurs within a relatively short timeframe (for example, rushing to a scene of an accident and filming).[213] It is generally not covert, with the exception of some forms of investigative journalism and filming for current affairs shows,[214] and celebrity photographers or 'paparazzi'.[215]

2.87 Nevertheless, in consultations it was suggested that photographers do not ask for permission to film people in public places, especially if the person is only part of the background of the picture.[216] Photographers may ask for permission, however, when they intend to use an image commercially, or for exhibitions.[217] Whether a photographer will seek permission to photograph may depend on whether the subject of the photograph knows that he or she is being observed.[218]

2.88 Media organisations indicated that there are restrictions on the activities that it can undertake in public places that are privately owned. For example, it was suggested that some shopping centres do not allow photographers to take photographs inside centres.[219] There are also restrictions on filming in places such as the courts and parts of some airports.[220]

180 David Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) 19 (2) *International Sociology* 135, 144.

181 These laws are discussed further in Chapter 5.

182 For an example of this approach see Council of Australian Governments, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (2006).

183 See, eg, *Security Improvement Program (SIP)*, Queensland Government <www.qld.gov.au/grants/grantdetails.action?grantId=8ae5936c063948ea01063949828e00a1> at 12 November 2008.

184 See Council of Australian Governments, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (2006).

185 Attorney-General's Department [Australia], *The National Security Hotline* <www.ag.gov.au/agd/www/nationalsecurity.nsf/Page/The_National_Security_Hotline> at 26 June 2008. Other non-terrorism hotlines include the Victorian State Government's 'Dob in a Hoon' hotline: Department of Justice [Victoria], *Dob in a Hoon: Hotline to Report Dangerous Drivers* <www.justice.vic.gov.au/wps/wcm/connect/DOJ+Internet/Home/About+Us/Media+Room/News+Archive/JUSTICE+-+Dob+in+a+Hoon:+Hotline+to+Report+Dangerous+Drivers+(NEWS)> at 12 November 2008; and the federal government's 'Immigration dob-in line': Department of Immigration and Citizenship [Australia], *Immigration Dob-In Line* <www.immi.gov.au/managing-australias-borders/compliance/staying-legally/dob-in-line.htm> at 12 November 2008.

186 Roundtables 13 and 20.

187 Roundtable 15.

188 Roundtable 15.

189 Roundtable 20.

190 Roundtable 13.

191 Roundtable 31.

192 Roundtable 31. See also *Mass Gatherings Infrastructure Assurance Advisory Group,* Trusted Information Sharing Network for Critical Infrastructure Protection <www.tisn.gov.au/www/tisn/tisn.nsf/Page/StructureoftheTISNInfrastructureAssuranceAdvisoryGroupsassGatheringsInfrastructureAssuranceAdvisoryGroup> at 12 November 2008.

193 Roundtable 20.

194 Roundtables 13 and 31.

195 Roundtable 31.

196 Roundtable 23.

197 Roundtable 19.

198 Roundtables 3.

199 Roundtables 7 and 8.

200 Roundtable 7.

201 Roundtable 31.

202 Roundtables 15 and 31.

203 Roundtable 31.

204 Roundtable 15.

205 Roundtable 20.

206 Roundtable 8.

207 Roundtable 19.

208 Roundtable 25.

209 Roundtable 25. See also *Case Note 2006: Complainant AE v Contracted Service Provider to a Statutory Authority [2006] VPrivCmr 6*, Office of the Victorian Privacy Commissioner <www.privacy.vic.gov.au/dir100/PriWeb.nsf/download/39948D727A2C2879CA2571C60083195D/$FILE/VPrivCmr%20%5B2006%5D%206.pdf> at 9 January 2009.

210 Roundtable 3.

211 Roundtable 25.

212 The commission notes that the Media Alliance Code of Ethics includes a direction to Alliance members engaged in journalism to 'commit themselves to…respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude': Media Entertainment and Arts Alliance, *Media Alliance Code of Ethics* (1999) <http://www.alliance.org.au/resources/media/> at 12 February 2009.

213 Roundtable 26.

214 Roundtable 27.

215 Roundtable 26.

216 Roundtable 26.

217 Roundtable 26.

218 Roundtable 26. As we noted in Chapter 1, the issue of non-consensual publication of photographs falls outside the scope of this reference because it is now the subject of a separate inquiry by the Standing Committee of Attorneys-General. See Standing Committee of Attorneys-General, Unauthorised Photographs on the Internet and Ancillary Privacy Issues Discussion Paper (2005).

219 Roundtable 26.

220 Roundtable 27.

Chapter 2 Current Practice

2.89 While the media engages in surveillance for newsgathering purposes, many media outlets use surveillance to gather information for stories with an entertainment focus. The Australian Privacy Foundation (APF) has highlighted that not all of the media's work is for 'public interest' purposes. The APF notes that it is important to distinguish between genuine news and current affairs journalism, and 'infotainment, entertainment and advertising.'[221]

2.90 A relatively new phenomenon which mirrors the development of the paparazzi is the 'snapperazzi': amateurs with mobile phones who follow celebrities and sell photographs of them to magazines.[222] One example involved a prison inmate who took secret photographs of jailed stockbroker, the late Renee Rivkin, while he was in prison.[223]

2.91 Finally, we learned that some media organisations share surveillance footage with police when required to do so by court order, and by agreement. In consultations, one group told the commission that it released footage to the police on average three times a week.[224]

LEISURE, ENTERTAINMENT AND OTHER PERSONAL USES

2.92 Public place surveillance is also used for personal leisure and entertainment purposes. People use hand-held cameras and video recorders to take family and holiday snapshots, or as amateur photography. People also use audio recording devices, including recorders contained in mobile phones or hand-held computers, to record lectures, presentations or important conversations.

2.93 Individuals may also use tracking devices in public places for personal purposes. Use of GPS technology in mobile phones and vehicles is now widespread. As the technology has standardised its cost has reduced, making it more widely accessible. Earlier in this chapter we gave other examples of GPS devices including their use by parents in children's clothing to trace a child's whereabouts[225] and the possibility of using devices, such as bracelets, to monitor those suffering from memory loss.[226]

MARKETING

2.94 Marketing is another driver of public place surveillance. An example is geo-identification (a form of data surveillance) which reveals the geographical location of an internet user (that is, the country or city in which they have logged on), allowing businesses using the technology to target locally appropriate products to the user.[227]

2.95 Earlier we referred to the example of an Australian marketing company giving its catalogue delivery workers a GPS device to collect information about households, such as whether fences need painting, which would then be on-sold to other businesses and advertisers,[228] and an Australian car-sharing program using GPS in its advertising-covered vehicles to report to those advertisers where members have driven their cars.[229]

2.96 Marketing research is also a driver.[230] For example, a new application of facial recognition and tracking devices allows supermarkets to use cameras to monitor and study customers' movements through the store, including how long they spend at particular aisles.[231]

TECHNOLOGY CREATING DEMAND

2.97 One further possible driver of public place surveillance is that the surveillance technologies themselves may be creating demand for their use.[232] Like all businesses, developers of surveillance technologies promote their products, and the latest technological gadgetry often entices potential users of surveillance.

2.98 Some writers have suggested that technology alone does not drive use of surveillance but that it builds on existing consumer interest. This is the view of Lyon who writes that 'the mere existence of new technologies is far from a sufficient reason for them to be used'. Rather, dramatic incidents, such as the September 11 attacks, coincide with active promotion of products, leading to sales. Lyon refers to 'high tech companies…wooing willing governments with their security and surveillance products' following the September 11 attacks.[233]

2.99 The different response to new surveillance technology by different countries is cited as evidence of the fact that technology alone does not create demand for surveillance. Lyon gives as an example the electronic identity card, which has gained acceptance in Thailand, Malaysia and Singapore, but has been rejected by Korea and is only just in planning stages in Canada, the UK and the US.[234] Benjamin Goold similarly discusses how the UK public received CCTV without much opposition in the early 1990s but there was a hostile reaction to CCTV in France and Germany in the same period.[235] The nature of the government and response from the community appear to be relevant factors when the utilisation of new mass surveillance technologies is considered.[236]

FUTURE TRENDS

2.100 Our terms of reference ask us to consider whether reform measures are necessary to control not only existing surveillance practices but also 'emerging methods of surveillance'.

2.101 Emerging methods of surveillance are difficult to describe comprehensively, because of the rapid pace of technological development. For example, when the Australian Law Reform Commission completed its report on privacy law in Australia in May 2008, attendees at a conference just five months later noted that 'cloud computing' had failed to make its way into the report.[237] 'Cloud computing' refers to a web-based computer operating system that allows an individual to merge their work computer, home computer and laptop into one online operating system so that each is accessible through the internet.[238] Another example is the 2006 Surveillance Studies Network reference to a surveillance practice that involves 'a virtual strip search using millimetre wave scanner[s]' at airports.[239] Today, just three years later, that technology is in piloted use in three of Australian airports.[240]

2.102 Observers have identified a number of future trends in surveillance technologies. These include:

- the increasing sophistication of devices and their expanding use
- the potential to facilitate greater control of mobility and access to places
- the potential to identify and target specific consumer behaviour
- greater use of behavioural surveillance and increased use of biometrics
- increasing convergence and connectivity of surveillance devices.

In the final part of this chapter we briefly discuss each of these trends.

221 Australian Privacy Foundation, *'Australia's Right to Know' Coalition: Independent Audit into the State of Media Freedom in Australia: Submission* (August 2007) 4.

222 Steve Dow, 'The Power of the Citizen Paparazzi', *The Sun Herald* (Sydney), 30 January 2005, 78.

223 Ibid.

224 Roundtable 27.

225 See, eg, 'GPS-equipped Jacket Lets Parents Track Their Children', *Sydney Morning Herald* (Sydney), 25 October 2007 <www.smh.com.au/news/technology/gpsequipped-jacket-lets-parents-track-their-children/2007/10/25/1192941200365.html> at 12 November 2008.

226 See Katina Michael, Andrew McNamee, MG Michael, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring' *Faculty of Informatics Papers,* University of Wollongong <ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers> at 21 May 2008.

227 Dan Svantesson, 'Geoidentification: A Serious Threat to Your Location Privacy on the Internet?' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

228 Simon Lauder, 'Junk Mail Deliverers to "Spy" on Households', *ABC News Online*, 23 May 2006 <www.abc.net.au/news/stories/2006/05/23/1645382.htm> at 11 November 2008.

229 *Car Advertising Benefits with Smartpilots Australia,* Smartpilots: Mobile Advertising and Communications <www.smartdrivers.com.au/sd/benefits.aspx> at 9 January 2009.

230 Brad Reed, *Study: Surveillance Software Revenue to Quadruple by 2013*, TechWorld (6 February 2008) <www.techworld.com.au/article/222912/study_surveillance_software_revenue_quadruple_by_2013?fp=4&fpid=229> at 20 January 2009.

231 Paul Redman, 'Measuring Customer Preferences and Needs with Traffic Pattern Analysis' (WO/2006/017132), http://www.wipo.int/pctdb/en/wo.jsp?IA=US2005024157&DISPLAY=DESC at 19 January 2009.

232 David Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) 19 (2) *International Sociology* 135, 141.

233 Ibid 136.

234 Ibid 141.

235 Benjamin Goold, *CCTV and Policing* (2004) 21-23.

236 David Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) 19 (2) *International Sociology* 135, 142.

237 *Cyberspace Law and Policy Centre Symposium, Meeting privacy challenges – the ALRC & NSWLRC Privacy Reviews*, Sydney, 2 October 2008.

238 See Galen Gruman, *What is cloud computing?* (16 June 2008) Information Age <www.infoage.idg.com.au/index.php/id;909486215;fp;4;fpid;10515158 1> at 10 December 2008; Asher Moses, 'Cloud Computing Takes the 'P' out of PC', *Sydney Morning Herald* (Sydney), 24 April 2008 <www.smh.com.au/news/technology/cloud-computing-takes-the-p-out-of-pc/2008/04/24/1208743109210.html> at 10 December 2008. Cavoukian suggests that cloud computing raises potentially serious privacy issues 'that come along with storing sensitive personal information in databases and software scattered around the Internet' see Ann Cavoukian (Information and Privacy Commissioner of Ontario), *Privacy in the Clouds — A White Paper on Privacy and Digital Identity: Implications for the Internet* 7 <www.ipc.on.ca/images/Resources/privacyintheclouds.pdf> at 10 December 2008.

239 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [28.3].

240 See, eg, Jano Gibson, 'Privacy Fears Over Airport Body Scan', *The Age* (Melbourne), 2 October 2008, 4; and Frances Stewart, 'Airport Trial: Passengers Face Fresh Search Security Scanner That Reveals it All', *The Advertiser* (Adelaide), 2 October 2008, 13.

Chapter 2 Current Practice

IMPROVED CAPACITIES

2.103 It is highly likely that technological advancements in other fields will make their way into devices that can be used to engage in surveillance in public places and that the trend towards greater sophistication of devices will continue. An example is the use of facial recognition technology in conjunction with CCTV systems. At the moment facial recognition technology is not in widespread use because of its limited capacity to accurately match faces to stored images. There are reports, however, that the technology is quickly improving.[241] In addition, it has been suggested that a number of other CCTV capabilities are likely to become cost-effective, including eavesdropping, lip-reading and x-ray cameras.[242]

MORE WIDESPREAD BUT LESS NOTICEABLE

2.104 Surveillance in public places is likely to become more widespread as devices become more affordable. In addition, surveillance is likely to become less noticeable. [243]

2.105 The ability to access surveillance technology is expanding. As we have seen, surveillance technology is increasingly being built into everyday products—for example GPS tracking capacities in motor vehicles[244] and in mobile phones.[245] In addition, surveillance users are increasingly likely to be private sector organisations and individuals as well as government. The Surveillance Studies Network predicts that the 'shift of power from public to private' will continue,[246] and refers to the example an outsourced transnational private consortium conducting border control in all EU member countries and the United States.[247] A local example drawn from consultations is the suggestion that some councils outsource the secure storage of their CCTV footage.[248]

2.106 While access to and use of surveillance devices is expanding, technological advances mean that public place surveillance is also becoming harder to detect. Advances in the areas of microchips and nanotechnology[249] have resulted in the manufacture of smaller and smaller surveillance devices. Cutting edge examples include miniaturised flying robotic devices with inbuilt video cameras which have been tested by engineers in the UK.[250] The United States Defense Advanced Research Projects Agency has reportedly conducted similar scientific trials involving insects. Called 'cyborgs', these live insects are implanted with surveillance devices and then controlled remotely by a human operator.[251] The covert nature of surveillance is accentuated by the rising number of military and commercial satellites,[252] with one of the best known being Google Earth.

CONTROLLING ACCESS AND MOBILITY

2.107 A further trend that has been identified is the increased use of surveillance to monitor public places in order to restrict entry to specific individuals or groups.[253] Some systems are highly visible and are negotiated willingly by users—for example those controlling Personal Identification Number (PIN) credit card purchases, airport passport control and gated communities.[254] While these systems operate to prohibit access to all but a small number of 'authorised people', increasingly, surveillance systems may also be used to restrict access based on less easily-definable characteristics.

2.108 For example, shopping centre managers in the UK have reported restricting entry of 'undesirable' people to shops because of particular personal characteristics including age, associations and perceived drug use.[255] These people were originally identified through CCTV systems, or by security personnel. Other people, targeted as a result of prior behaviour, were granted entry into a centre but were subject to 'surveillance and assessment' while on the premises.[256]

2.109 There are also more covert types of surveillance designed to distinguish between people in order to control access. Such surveillance systems include those designed to sort internet or call centre traffic, allowing certain people's traffic to be sped-up whilst slowing down or blocking other callers. As Stephen Graham and David Murakami Wood note, 'such stealthy passage points force users to unknowingly negotiate surveillance as a hidden background to their everyday life and movement.'[257]

TARGETED ADVERTISING

2.110 The trend towards the use of surveillance to identify and target specific consumer behaviour is also likely to continue in the future.[258] For example, surveillance is used to collect detailed 'information about individuals' interests, actions, habits, and traits' with a view to tailoring advertising to individual consumers.[259] Collection of personal information for this purpose has been controversial. Internet service providers in the UK have come under criticism for plans to track the internet activities of their customers in order to provide targeted advertising.[260]

2.111 Schemes such as this will have more extensive privacy ramifications once the use of RFID technology becomes more widespread. For example, an IBM patent filed in 2001 and granted in 2006 refers to the potential to incorporate networked RFID readers called 'person tracking units' via their use of 'credit card, bank card, shopper card or the like.'[261] Each card would contain an embedded microchip, and microchip readers would be installed in places where people regularly go, such as train stations, supermarkets, shopping centres and airports.[262] The reader would register each time that person's microchipped card passes by, thus effectively tracking its owner[263]and providing valuable marketing information.

2.112 A potential application of mobile phone tracking technology is use by mobile phone service providers to track the location of customers and send advertising messages targeted to the customer's location[264] (for example, a text message containing movie trailers for a movie theatre in the vicinity of the text message recipient).[265] It has been suggested that in the future, people might expressly consent to this form of tracking in return for a lower mobile phone service fee.[266]

BEHAVIOURAL MONITORING

2.113 It has also been observed that we may see new forms of behavioural surveillance based on behaviour recognition technology (without the need for operator input) in the future. For example, a video interpretation system trialed in the Barcelona metro demonstrated a high level of success in recognising specific behaviours including fraud and vandalism. Detailed camera images may potentially be combined with computer software to determine the mental state and likely future behaviour of people.[267] It has been suggested that scanning faces in a crowd for telltale expressions associated with specific mental states such as rage may be used to predict violent behaviour.[268]

241 See, eg, R. Jenkins* and A. M. Burton, *100% Accuracy in Automatic Face Recognition,* Science (25 January 2008) <www.sciencemag.org/cgi/content/abstract/319/5862/435> at 10 December 2008.

242 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [6.66].

243 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [26.2] and [34.3].

244 Office of the Victorian Privacy Commissioner, *Privacy Aware* Vol 3, No 1 (2004) 5; see also Office of the Victorian Privacy Commissioner, 'Privacy and the Car' (Press Release, 8 April 2004) <www.privacy.vic.gov.au/dir100/priweb.nsf/download/1772740D4AF8C509CA256E70001863BD/$FILE/media_8.4.04_web.pdf> at 10 December 2008.

245 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info Sheet 05.03 (2003).

246 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [26.2].

247 Ibid [27.1].

248 Roundtable 7.

249 A Delbridge, et al (eds) *The Macquarie Dictionary* (revised 3rd ed) (2001) 1270 defines 'nanotechnology' as 'technology which relates to the manufacture of microscopic objects'.

250 See Chris Riley, *Robotic Insect Takes to the Air* (11 April 2001) BBC News <news.bbc.co.uk/1/hi/sci/tech/1270306.stm> at 10 December 2008.

251 See Sophie Borland, 'Insect 'spies' fitted with video camera implants', *Telegraph* (London), 6 March 2008 <www.telegraph.co.uk/earth/main.jhtml?xml=/earth/2008/03/06/scirobot106.xml> at 10 December 2008.

252 Patrick Korody, 'Satellite Surveillance Within US Borders' (2004) 65 *Ohio State Law Journal* 1627.

253 See John Flint, 'Surveillance and Exclusion Practices in the Governance of Access to Shopping Centres on Periphery Estates in the UK' (2006) 4 (1/2) *Surveillance and Society* 52.

254 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) Appendix 4: Stephen Graham and David Murakami Wood, 'Expert Report: Infrastructure and Built Environment' 2.

255 John Flint, 'Surveillance and Exclusion Practices in the Governance of Access to Shopping Centres on Periphery Estates in the UK' (2006) 4 (1/2) *Surveillance and Society* 52, 54 and 60.

256 Ibid 60.

257 Ibid Appendix 4: Stephen Graham and David Murakami Wood, 'Expert Report: Infrastructure and Built Environment' 2.

258 *Privacy Topics: Behavioural Targeting,* Privacy International (2007) <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559082&als[theme]=Privacy%20and%20Human%20Rights> at 9 January 2009.

259 Ibid.

260 See Charles Arthur, 'Phorm Fires Privacy Row for ISPs', *Guardian* (London), 6 March 2008 <www.guardian.co.uk/technology/2008/mar/06/internet.privacy> at 10 December 2008.

261 Katherine Albrecht, 'How RFID Tags Could Be Used to Track Unsuspecting People', *Scientific American Magazine* (August 21 2008) <www.libertycoalition.net/how-rfid-tags-could-be-used-track-unsuspecting-peo> at 10 December 2008.

262 Ibid.

263 Ibid.

264 Anick Jesdanun, 'Wherever You Go, Ads are Sure to Follow', *The Advertiser* (Adelaide), 4 January 2008, 19.

265 'Mobile ads: a threat to your privacy?', Australian Associated Press, 3 January 2008 <http://m.cnet.com.au/mobilephones/339284809.htm> at 9 December 2008 .

266 Rob Nicholls, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

267 Carole Smith, 'Hacking the Mind' (2007/2008) 25 *Dissent* 46 See also: Carole Smith, *Intrusive Brain Reading Surveillance Technology: Hacking the Mind* (2007) Global Research: Centre for Research on Globalization <www.globalresearch.ca/index.php?context=va&aid=7606> at 9 December 2008.

268 See Malcolm Gladwell, 'The Naked Face', *The New Yorker* (New York), 5 August 2002, 38–49.

Chapter 2 Current Practice

2.114 A project called iBox, developed by National Information and Communication Technology Australia, converts analogue video data into a digital format which is then analysed using complex algorithms to interpret physical characteristics, appearances and mannerisms so to identify suspicious behaviour.[269]

INCREASED USE OF BIOMETRICS

2.115 Biometrics[270] may be used more extensively in the future for both authentication and identification.

2.116 Authentication is the act of verifying that a person is who they claim to be.[271] A range of biometrics, including fingerprints and retinal and iris scans, may eventually replace traditional methods of authentication, such as signatures and passwords, as they become cheaper and more reliable. Authentication is generally used for access control purposes and relies on a databank of comparative information against which the biometric material can be compared.

2.117 Biometrics such as fingerprints and DNA are now used extensively by law enforcement bodies to identify possible crime suspects and there is pressure to expand the collection of DNA with a view to establishing more extensive databanks.[272] At the same time the use of facial recognition technology is likely to accelerate the identification of people who are filmed via CCTV, camera phones or traditional cameras.[273]

CONVERGENCE AND CONNECTIVITY

2.118 Behavioural monitoring and targeted advertising are examples of a broader trend towards the convergence of surveillance systems. Kevin Haggerty and Richard Ericson describe a 'convergence of what were once discrete surveillance systems to the point that we can now speak of an emerging "surveillance assemblage"'.[274] They suggest that in the modern world 'surveillance is driven by the desire to bring systems together…to integrate them into a larger whole'.[275] We are now able to talk about entire 'surveillance systems' which combine surveillance and data gathering capabilities.[276]

2.119 The trend towards merging devices and data sources is likely to continue. Increasing use of digital technology is accelerating this trend. Once images are in digital form the potential to link those images with other databases increases dramatically.[277] Norris has noted, for example, that digital CCTV systems are likely to be put to greater use:[278]

> *CCTV systems can be integrated with automated access control systems. For instance at a leisure center a digital database of those who have paid their subscriptions can be linked to the cameras monitoring the turnstile so that facial recognition software can determine whether the person is entitled to access. Similar technology on the metro could ensure that passengers convicted of assaulting members of staff are identified and barred from passing through the automated gates.*[279]

2.120 In a recent conference paper computer science academics describe a vision of the future, referred to as 'ubiquitous computing' or 'ambient intelligence', in which:

> *humans will be surrounded by intelligent interfaces that are supported by computing and networking technology embedded in all kinds of objects in the environment and that are sensitive and responsive to the presence of different individuals in seamless and unobtrusive way. This assumes…that computing will move to the background, weave itself into the fabric of everyday living spaces and disappear from the foreground, projecting the human user into it.*[280]

2.121 Suggested cutting-edge capabilities of this new technology include new uses for mobile phones with the capability of displaying information about people 'by means of machine vision'. A phone could be directed at a product bar code or RFID tag and give the user details about the product including its attributes, origin, price, warranty and reviews.[281]

2.122 Another example of 'ubiquitous computing' is provided by research conducted at the University of Virginia:

> *The University of Virginia's AlarmNet research project has interconnected networks with some everyday things such as beds and floors. A pressure sensor in a bed detects heart rate, breathing and movement; sensors in the floor nearby can detect when a person falls…Pressure sensors in beds or furniture may also be able to detect sudden weight gains associated with certain heart conditions and the side effects of beta blockers.*[282]

2.123 The consequences of the convergence of surveillance technologies include a greater ability of surveillance users to compile detailed pictures of the public.[283] It also increases 'the risk of "surveillance creep" as multiple uses are found for technologies and as information gathered for one purpose or in one domain leaks through into others'.[284]

2.124 Haggerty and Ericson suggest that this convergence or networking of surveillance technologies creates a 'knowledge of the population [which] is now manifest in discrete bits of information which break the individual down into flows for purposes of management, profit and entertainment'.[285] They suggest that this convergence of surveillance technologies and data flows makes it 'increasingly difficult for individuals to maintain their anonymity'.[286]

CONCLUSION

2.125 This chapter reveals that public place surveillance is widespread in Victoria. Many surveillance technologies that were once only used by the military and police are now available to businesses and individuals.

2.126 The widespread use of public place surveillance means that we can no longer assume that activities performed in public places will pass unobserved and unrecorded. Like many other modern societies, ours is a 'surveillance society' and, as noted by the UK Surveillance Studies Network, 'it is pointless to talk about surveillance society in the future tense'. While it is impossible to predict the technological advances that lie ahead, this reference provides us with an opportunity to assess community responses to the significant recent technological developments.

2.127 There are many important purposes served by public place surveillance in Victoria, including safety, crime prevention and control, journalism and entertainment. Many Victorians have a stake in the continued use of surveillance technology, including police, local councils, transport operators, sporting and entertainment venues, retailers, private investigators, journalists and individuals. All Victorians have a stake in ensuring that surveillance technology is used responsibly so that everyone may continue to enjoy public places.

269 *Aussie Video Surveillance Technology Leaves Rivals for Dead*, Electrical Contractor: Power and Integrated Building Systems <www.ecmag.com/index.cfm?fa=article&articleID=7385> at 10 December 2008.

270 Biometrics may be described as the 'automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odors': *Biometrics: Who's Watching You?,* Electronic Frontier Foundation (September 2003) <www.eff.org/wp/biometrics-whos-watching-you> at 10 December 2008.

271 *Authentication and Identity Disclosure* (2007) Privacy International <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559076> at 2 February 2009.

272 *Genetic Privacy* (2007) Privacy International <www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559080> at 2 February 2009.

273 Tom Geoghegan, 'How Your Face Could Open Doors', *BBC News* (Glasgow, UK), 25 November 2004 <http://news.bbc.co.uk/1/hi/magazine/4035285.stm> at 2 February 2009.

274 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 (4) *British Journal of Sociology* 605, 606.

275 Ibid 606.

276 For further discussion on the linking of location devices and information databases see: Roger Clarke and Marcus Wigan, 'You are Where You Have Been' in Katina Michael and M G Michael (eds), *Australia and the New Technologies: Evidence Based Policy in Public Administration* (2008) 100.

277 Clive Norris, 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control' in David Lyon (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (2003) 269.

278 Ibid 249, 275.

279 Ibid 249, 275.

280 Maja Pantic et al, 'Human Computing and Machine Understanding of Human Behavior: A Survey' in *Proceedings of the 8th international conference on Multimodal interfaces* (2006) <www.doc.ic.ac.uk/~maja/PanticEtAl-ICMIposition-FINAL.pdf> at 10 December 2008.

281 National Intelligence Council [US], *Disruptive Technologies Global Trends 2025*, Appendix F: The Internet Of Things (Background) 10. <www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf> at 10 December 2008.

282 Ibid.

283 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008)136.

284 Ibid 139.

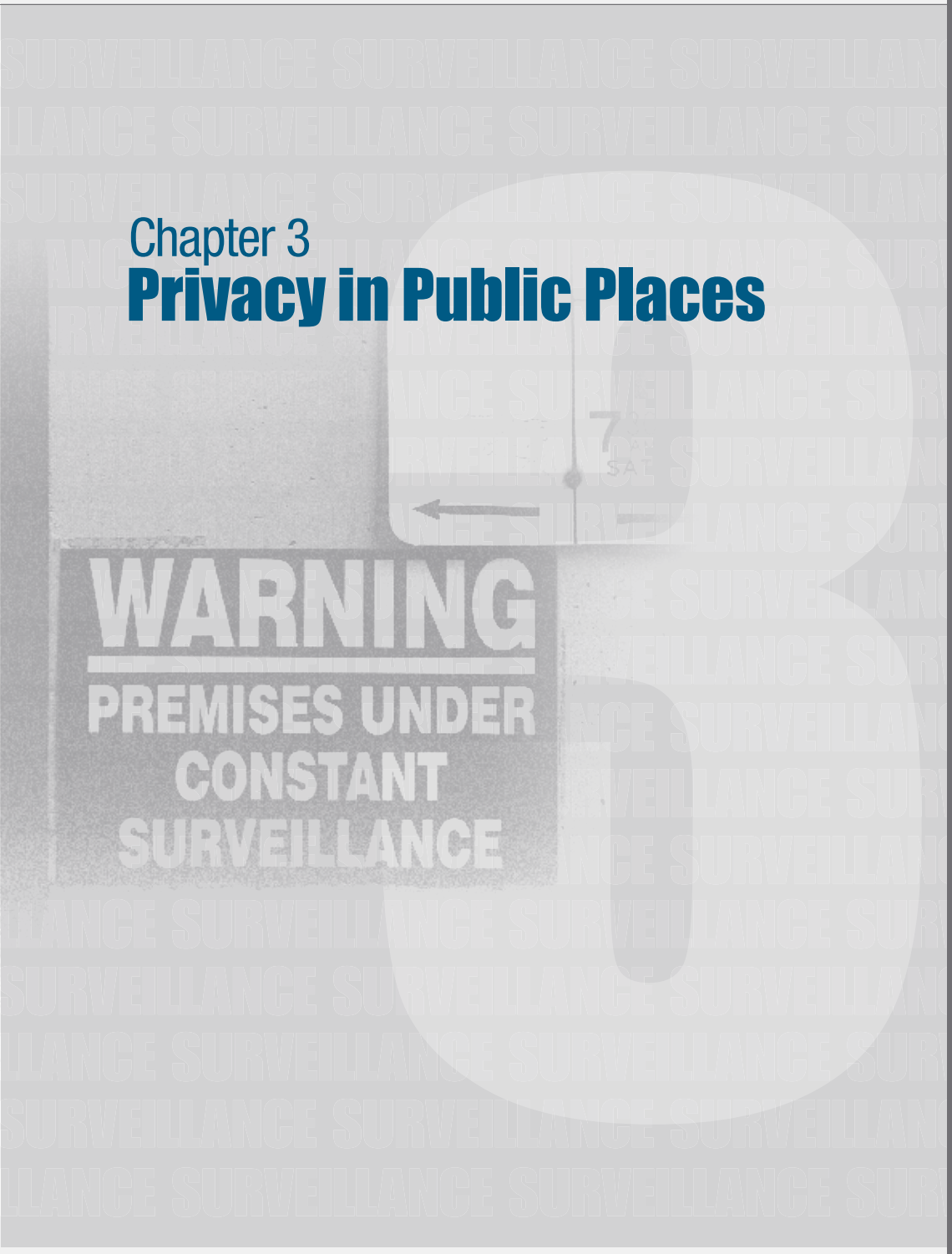
285 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 (4) *British Journal of Sociology* 605, 619.

286 Ibid 619.

Chapter 2 Current Practice

Chapter 3

Privacy in Public Places



Chapter 3

Privacy in Public Places

INTRODUCTION

3.1 The terms of reference require the commission to consider 'the protection of privacy, autonomy and dignity' when considering 'whether legislative or other measures are necessary to ensure that there is appropriate control of surveillance' in 'places of public resort'. We begin this task by examining the concept of privacy and its connection with the human values of autonomy and dignity.

WHAT IS PRIVACY?

3.2 The word privacy comes from the Latin root 'privare' meaning to separate.[1] The *Macquarie Dictionary* defines privacy as 'the state of being private; retirement or seclusion' and 'secrecy'.[2]

3.3 In our Occasional Paper *Defining Privacy* (published as part of the Workplace Privacy reference), we referred to privacy 'as always involving a boundary, which is transgressed in any breach of privacy'.[3] Similarly, Privacy International has written that 'privacy protection is frequently seen as a way of drawing a line at how far society can intrude into a person's affairs'.[4]

CONCEPTUALISING PRIVACY

3.4 Despite the fact most people have some familiarity with the concept of privacy, expert commentators report that defining privacy is a difficult, and perhaps impossible, task. This is due to the breadth of the concept of privacy. It covers several overlapping notions, including secrecy, confidentiality, solitude of the home, control over information about oneself, and freedom from surveillance.[5]

3.5 Over one hundred years ago, influential commentators described privacy as 'the right to be let alone'. While the origins of this description lie in a treatise on torts by US Judge Thomas Cooley, it gained currency when used in a seminal article by Louis Brandeis and Samuel Warren to define what they meant by privacy when arguing for its protection under the common law of the US.[6] Many years later, in *Time, Inc v Hill*, US Supreme Court Justice Fortas described the 'right to be let alone' as the right 'to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law'.[7]

3.6 Another common view of privacy is that it is concerned with secrecy.[8] Privacy is violated when there is 'public disclosure of previously concealed information'.[9] However, some writers have criticised the view of privacy as secrecy, noting that people are often less concerned with keeping information completely from public view than in controlling who has access to that information. For example, Daniel Solove has written about users of the internet-based social networking site Facebook who took issue with its News Feeds feature sending notices to their 'friends' when their profiles had been changed. The users found it to be an invasion of privacy, despite the fact that their profiles were otherwise accessible, to friends and other extended networks. According to Solove, these individuals:

> *considered the issue as a matter of accessibility. They figured that most people would not scrutinize their profiles carefully enough to notice minor changes and updates.*[10]

3.7 A third view of privacy is that it involves peoples' ability to limit access to themselves. Ruth Gavison has said that privacy is, at its simplest, the ability to:

- limit information others have about you (secrecy)
- ensure that others do not pay attention to you (anonymity)
- limit physical access by others to yourself (solitude).[11]

Solove suggests that the conception of privacy as limiting access to oneself is closely associated with (and a more sophisticated version of) privacy as the 'right-to-be-let-alone'.[12]

3.8 A fourth and influential view of privacy is that it involves the control of personal information.[13] This view is influential because it is the foundation of information privacy or data protection laws enacted in numerous countries, including Australia.[14] Alan Westin has described privacy as the ability of persons 'to determine for themselves when, how, and to what extent information about them is communicated to others'.[15]

3.9 Also influential is the personhood concept of privacy, which sees privacy as primarily about the freedom for individuals to give expression to themselves.[16] In particular, the personhood theory of privacy regards privacy as protecting individuality, dignity and autonomy.[17] For example, in the recent UK privacy case *Mosley v News Group Newspapers Ltd*, Justice Eady identified the purpose of the law's protection of privacy, to be 'to prevent the violation of a citizen's autonomy, dignity and self-esteem'.[18] In Australia, members of the High Court have associated privacy with dignity and autonomy. In *Australian Broadcasting Corporation v Lenah Game Meats*, Chief Justice Gleeson wrote that 'the foundation of much of what is protected, where rights of privacy, as distinct from rights of property, are acknowledged, is human dignity'.[19] Justices Gummow and Hayne[20] described privacy 'as a legal principle drawn from the fundamental value of personal autonomy', quoting from the Lord Justice of Appeal Sedley in the UK case *Douglas v Hello! Ltd*.[21] As a theory, the personhood theory of privacy is more about why we value privacy, than what privacy is. [22]

3.10 Anonymity is the ability to remain anonymous or unknown. It has been described as one form of privacy, linked to the value of autonomy. Moreover, anonymity has been traditionally associated with public places. Westin writes that anonymity occurs:

> *when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him.[23]*

3.11 Finally, there is a view that privacy involves intimacy. Specifically, privacy is necessary to create the conditions for the development of personal relationships.[24] The notion that privacy is concerned with intimate relationships is evident in judgments of the European Court of Human Rights. In *X v Iceland*, the court said that the right to privacy includes 'the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality'.[25] Julie Inness has more broadly argued in *Privacy, Intimacy, and Isolation* that privacy covers 'intimate information, access, and decisions'.[26]

1 Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005) [1.32].

2 A Delbridge, et al (eds) *The Macquarie Dictionary* (revised 3rd ed) (2001) 1511.

3 Kate Foord, *Defining Privacy* (2002) 5.

4 *Overview of Privacy,* Privacy International citing Simon Davies <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559474> at 24 November 2008.

5 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1088; *Overview of Privacy,* Privacy International citing Ruth Gavison <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559474> at 24 November 2008; and New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.55].

6 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 (5) *Harvard Law Review* 194, 195.

7 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1101 citing *Time, Inc v Hill* (1967) 385 US 374, 413 (Fortas J dissenting).

8 Ibid 1105.

9 Ibid 1105.

10 Daniel Solove, 'The End of Privacy?' (2008 September) *Scientific American* 79, 82.

11 Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89 (3) *Yale Law Journal* 421, 428.

12 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1102.

13 Ibid; New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.17].

14 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008)[2.17].

15 Alan Weston, *Privacy and Freedom* (1967) 7.

16 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.24].

17 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1118.

18 *Mosley v New Group Newspapers Ltd* [2008] EWHC 1777 (QB) [7].

19 *Australian Broadcasting Corporation v Lenah Game Meats Pty* Ltd (2001) 208 CLR 199, 226 (Gleeson CJ).

20 *Australian Broadcasting Corporation v Lenah Game Meats Pty* Ltd (2001) 208 CLR 199, 251 (Gummow and Hayne JJ).

21 *Douglas v Hello! Ltd* [2001] QB 967, 1001 (Sedley LJ).

22 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1118.

23 Alan F Westin, *Privacy and Freedom* (1967) 31.

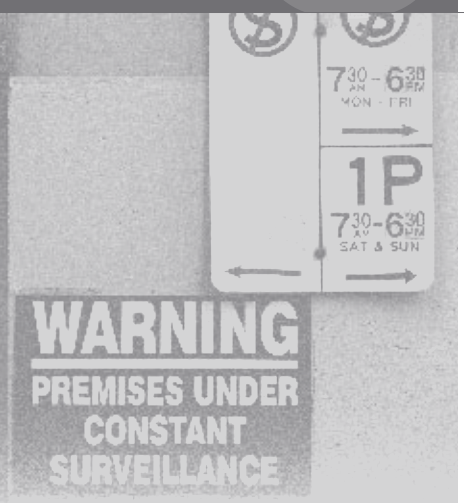
24 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008)[2.26].

25 *X v Iceland* (1976) 5 Eur Court HR (ser A) 87.

26 Julie Inness, *Privacy, Intimacy, and Isolation*, (1992) 56.

Chapter 3

Privacy in Public Places



ARGUMENTS AGAINST A SINGLE DEFINITION

3.12 The various attempts to conceptualise privacy have been criticised. For example, Solove has written that all the theories suffer from being either too narrow or too broad; they either fail to capture aspects of life normally deemed private, or capture those not normally deemed private.[27] As a result, some commentators have asked whether there is a core to privacy that is definable, or whether in fact there is no central part to the various interests we group together and seek to understand as privacy.[28] As Solove has argued, privacy is a 'sweeping concept' and a single definition may 'not fit well when applied to the multitude of situations and problems involving privacy'.[29] Solove proposes a pragmatic approach by focusing on privacy problems, which he defines as disruptions to certain practices. These practices may include letter writing, talking to a psychotherapist and engaging in sexual intercourse.[30] Thus, 'privacy violations consist of a web of related problems that are not connected by a common element, but nevertheless bear some resemblances to each other'.[31]

3.13 Other law reform commissions have noted the value of Solove's pragmatic approach when considering public policy and law reform.[32] For example, the Australian Law Reform Commission (ALRC), in its examination of privacy law in Australia, concluded that it would adopt Solove's pragmatic approach rather than try to characterise privacy by finding 'common denominators that make things private'.[33] According to the ALRC, it is possible to conduct law reform analyses without an 'overarching definition of privacy'.[34]

3.14 The New Zealand Law Commission (NZLC), after an extensive review of the work of privacy theorists, adopted a dual approach to the issue of definition. It opted for a 'harms to privacy' approach[35] that borrows from Solove's pragmatic approach[36] and also a 'core values' approach, identifying 'autonomy' and 'equal entitlement to respect' as core values.[37]

PRIVACY INTERESTS

3.15 Another approach to conceptualising privacy is to consider it as a 'bundle' of disparate 'interests'.[38] For example, Raymond Wacks suggests that privacy is valued ''because of the interests embedded and enabled by it'.[39] *In Lenah Game Meats,* Chief Justice Gleeson referred to 'interests of a kind which fall within the concept of privacy'.[40]

3.16 Four interests are commonly referred to when discussing privacy:

- territorial privacy, or the interest in controlling entry into one's personal space
- bodily privacy, or the interest in freedom of interference with one's person
- information privacy, or the interest in controlling information held by others about oneself
- communications privacy, or the freedom from interception of one's communications.[41]

3.17 Various common and emerging forms of surveillance have the capacity to interfere with all four interests.[42] For example, surveillance footage obtained by closed-circuit television (CCTV) or satellite imagery may interfere with a person's interest in controlling personal space (territorial privacy). Biometrics, such as iris scans and facial recognition technology, may interfere with a person's bodily privacy. Tracking devices may interfere with a person's interest in controlling information about them, such as their location at a given moment (information privacy), and listening devices have the capacity to interfere with privacy of communications.

VARIATION OVER TIME AND BY CULTURE

3.18 What constitutes privacy differs over time and between people of different ages and from different cultures.[43] The ALRC described people's different expectations of privacy in its initial privacy report:

> *Some people hate to receive junk mail. Others, the Commission has found, delight in receiving it. Indeed, it is for them a valued contact with the outside world. Some people wish their health details to remain strictly private and are strongly against use of these details even by medical researchers. Others welcome such use. Some will even sell their abnormal medical histories, or those of members of their family, to the mass media, for publication to the community at large.*[44]

3.19 Matters widely considered as private clearly change over time. For example, Brett Mason has suggested that views have changed about the extent to which a person's sexuality is a private matter.[45] In the same vein, there is a widely held view that young people have different views than their parents' generation about matters that are private, as evidenced by the information young people share on the internet.[46] A survey by the Office of the Privacy Commissioner in 2007 found that younger Australians are less concerned about providing their financial information than relating their home telephone and address.[47] Younger Australians were also more concerned about CCTV.[48] A European wide survey similarly found that young people were more opposed to CCTV and more likely to believe that cameras were influencing their behaviour.[49]

3.20 What is private can also vary by context and culture. In our Occasional Paper, *Defining Privacy*, we wrote that what is considered private in the workplace may be more freely shared outside of the workplace.[50] James Whitman has compared understandings of privacy in the United States with those in Europe.[51] According to Whitman, 'American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity.'[52] Whitman suggests that in the United States privacy is regarded as freedom from intrusion by the state, and especially, intrusions into the home. By way of contrast, in Europe privacy is regarded as the right to control information about yourself and to control the way in which others see you to avoid embarrassment or humiliation. Even within Europe, there is variation in attitudes towards privacy. The Europe-wide survey, referred to above, found that 90 per cent of respondents in London viewed open street CCTV as a good thing, but only 25 per cent of respondents in Vienna shared that view.[53]

27 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1094.

28 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.3]. The ALRC and NZLC have noted that this pragmatic approach to privacy that focuses on privacy relevant practices, rather than an overarching definition, is more amenable to law reform. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.67]-[1.68]; New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [3.2].

29 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1088, 1099.

30 Ibid 1129.

31 Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 759.

32 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.67]; New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.16]-[2.17].

33 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.62].

34 Ibid [1.67]-[1.68].

35 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008)[3.9].

36 The harms include various interferences with privacy, such as intrusions into one's solitude, 'interference with one's peace of mind, intrusion upon an individual's solitude or loss of control over facts about oneself': Ibid [3.9].

37 Ibid [3.10].

38 Cf 'rights'. The ALRC suggests that 'while privacy is a 'right' in the legal sense, for definitional purposes, the word "interest" may be more accurate. A right is always an interest, even if not all interests are afforded the status of legal rights': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008)[1.56].

39 Kate Foord, *Defining Privacy* (2002) 10 citing Raymond Wacks, *Law, Morality and the Private Domain* (2000) 240-241.

40 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* 208 CLR 199, 225 (Gleeson CJ).

41 Australian Law Reform Commission, *Privacy* Report No 22 (1983) [46]; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.31].

42 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [1.5].

43 Kate Foord, *Defining Privacy* (2002) 5.

44 Australian Law Reform Commission, *Privacy* Report No 22 (1983) [21].

45 Brett Mason, *Privacy Without Principle: The Use and Abuse of Privacy in Australian Law and Public Policy* (2006) 83-84.

46 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.66].

47 Wallis Consulting Group Pty Ltd, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner* WG3322 (2007) 24.

48 Ibid 74.

49 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 9.

50 Kate Foord, *Defining Privacy* (2002) 5.

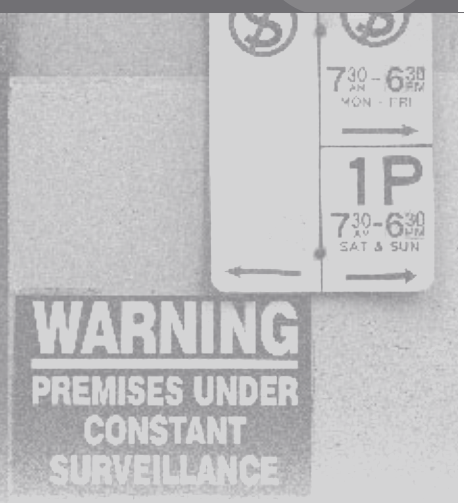
51 James Whitman, 'Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) *Yale Law Journal* 1151.

52 Ibid 1151, 1163.

53 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 8.

Chapter 3

Privacy in Public Places



OUR APPROACH TO PRIVACY

3.21 In *Defining Privacy* we proposed a working definition of privacy drawn from the values privacy seeks to protect.[54] In particular, we identified privacy as the right:

- not to be turned into an object or thing
- not to be deprived of the capacity to form and develop relationships.[55]

The first arm relies on the notions of personhood, autonomy and dignity, while the second relies on the notion of privacy as intimacy.

3.22 In keeping with the pragmatic approach advocated by Solove, and now adopted in part by two other law reform bodies,[56] we suggest that privacy involves many concerns and interests. A single definition of privacy is not necessary for us to consider whether people's privacy is threatened by the growing use of surveillance in public places.

HOW IMPORTANT IS PRIVACY?

3.23 Why do we need privacy protection? Some writers have suggested that privacy may not be a particularly important human need. Observers have noted that societies with less privacy have flourished.[57] Some argue that too much emphasis on privacy may be bad for society. For example, Heinz Arndt has written that privacy promotes individualism and antisocial behaviour.[58] Another view is that privacy is a form of concealment and deception, and allows people to be hypocrites, showing one face in public and another in private.[59] Amitai Etzioni has said that while privacy is an important value, it has probably received too much weight as against other interests,[60] and Mirko Bagaric has similarly said that a concern for privacy prevents societies from pursuing important aims such as safety and security.[61]

3.24 It is highly likely, however, that few people would dispute the suggestion that privacy is essential in a range of every day matters, such as banking, business, diplomacy, health care and interpersonal relationships.[62] In addition, most people would be very distressed if they had to undress, wash, or use the toilet in public.

3.25 Some writers have sought to describe the benefits that flow from protecting privacy. Roger Clarke has outlined four broad types of benefit:

1. psychological, by ensuring private space
2. sociological, by allowing people the freedom to behave as they wish and associate with others
3. economic, by allowing people freedom to innovate
4. political, by allowing people to think freely and argue.[63]

3.26 Some people suggest that 'privacy doesn't matter until it does'[64]—the point being that we are usually not concerned with privacy in the abstract, but only with specific instances when privacy is threatened. When privacy is breached, however, it is generally not reparable. For example, once private information becomes public it cannot be made private again.

PRIVACY AS A HUMAN RIGHT

3.27 Perhaps the strongest evidence of the contemporary importance of privacy is its growing legal significance and its elevation to the status of a human right. Early recognition of privacy is found in the Qur'an, the sayings of Mohammad, and the Bible, while Jewish law recognises 'the concept of being free from being watched'.[65]

3.28 Legal developments in the 18th and 19th centuries, in countries such as the UK, France, Sweden and Norway, included regulations affecting peeping Toms, eavesdroppers, warrantless seizures of papers, publication of private facts, and government handling of personal information.[66] The 1890 Warren and Brandeis article we have mentioned[67] contributed to the development of both a common law and a constitutional right to privacy in the United States.[68]

3.29 Major international and domestic human rights instruments developed in the 20th century include the right to privacy. For example, Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) states:

> 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.[69]

Article 12 of the *Universal Declaration of Human Rights*[70] refers to privacy in almost identical terms, and Article 16 of the *Convention on the Rights of the Child* applies these terms to the rights of children.[71]

3.30 Many countries include a right to privacy in their constitution.[72] Section 13 of the Victorian *Charter of Human Rights and Responsibilities Act 2006* (the Charter) includes the right to privacy in terms almost identical to those in Article 17 of the ICCPR.[73] Like most other human rights, the right to privacy in the Charter is not absolute and may be limited in some circumstances after balancing the various interests at stake.[74]

3.31 A tort of invasion of privacy is in the process of development in a number of common law countries. Courts in New Zealand have accepted the existence of the tort, while in the UK the action for breach of confidence has expanded to cover a range of privacy infringements.[75] It has been suggested that a tort of invasion of privacy in the UK may emerge from this body of case law. In Australia, two lower court decisions have recognised a right to privacy.[76] The High Court has given an indication that it may develop a right to privacy as part of the common law of Australia.[77]

PRIVACY AS A SOCIAL VALUE

3.32 It has been suggested that privacy is a social value as well as an individual human right. This view was proposed many years ago by John Dewey[78] who argued that the wellbeing of individuals and society were interrelated.[79] Solove, for example, says that 'a society without privacy protection would be suffocating, and it might not be a place in which most would want to live'.[80]

54 Kate Foord, *Defining Privacy* (2002) 1.

55 Ibid 27.

56 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [3.10]; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.54]-[1.68].

57 Australian Law Reform Commission, *Privacy* Report No 22 (1983)[34] citing Richard Posner, 'The Right to Privacy' (1978) 12 *Georgia Law Review* 393, 407.

58 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [2.47] citing Heinz Arndt, 'The Cult of Privacy' (1949) 21 *Australian Quarterly* 69-71.

59 Ibid [2.49].

60 Ibid Amitai Etzioni, *The Limits of Privacy* (1999) 7.

61 Mirko Bagaric, 'Privacy is the Last Thing We Need', *The Age* (Melbourne), 22 April 2007 <www.theage.com.au/news/opinion/privacy-is-the-last-thing-we-need/2007/04/21/1176697146936.html#> at 25 November 2008.

62 Peter Brown, 'Privacy in an Age of Terabytes and Terror' (2008 September) *Scientific American* 24, 24.

63 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [1.39].

64 Roger Clarke, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008). The ALRC has proposed in its recently issued report on privacy law in Australia that there be a longitudinal study of the attitudes of Australians towards privacy: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [67.96].

65 *Overview of Privacy,* Privacy International, <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559474> at 24 November 2008.

66 Ibid.

67 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 (5) *Harvard Law Review* 194.

68 In particular, as Supreme Court judge, Brandeis would later famously dissent in *Olmstead v United States* where the Court held that wiretapping was not a violation of the Fourth Amendment's prohibition on warrantless searches, there being no physical trespass of the home. *Olmstead v United States*, 277 US 438 (1928). *Olmstead* was overturned by *Katz v United States*, 389 US 347 (1967).

69 *International Covenant for Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). The *Privacy Act 1988* (Cth) gives effect to Australia's obligations under Article 17 of the ICCPR.

70 GA Res 217 A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/RES/217A (10 December 1948).

71 Opened for signature 20 November 1989, 1577 UNTS 44, (entered into force generally 2 September 1990).

72 *Overview of Privacy*, Privacy International <www.privacyinternational.org/article.shtml?cmd[347]=x-347-559474> at 24 November 2008.

73 United Nations, *International Covenant on Civil and Political Rights* Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966: entry into force 23 March 1976, in accordance with Article 49 . Section 13 of the Charter defines the right to privacy as the right of a person 'not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with'. Article 17 of the ICCPR states in part: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence …'

74 This matter is discussed further in Chapter 5.

75 See, eg, *Hosking v Runting* [2003] 3 NZLR 285. In the UK decision *Mosley v New Group Newspapers Ltd* [2008] EWHC 1777 (QB) Eady J comments that 'now (and especially since the formulation by Lord Nicholls in *Campbell v MGN Ltd* [2004] 2 AC 457) it is common to speak of the protection of personal information…without importing the customary indicia of a duty of confidence. The question arises whether it may now be correct to apply the label "tort" to this expanded cause of action'.

76 *Grosse v Purvis* [2003] QDC 151 and *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281.

77 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 248-9 (Gummow and Hayne JJ). This case is discussed further in Chapter 5.

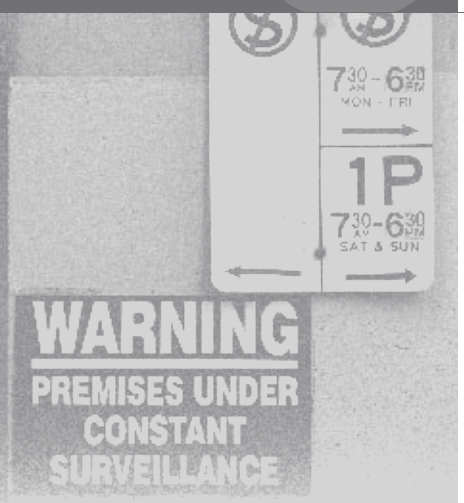
78 Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 762 discussing John Dewey, *Liberalism and Civil Liberties* (1936).

79 Ibid 762.

80 Ibid 762.

Chapter 3

Privacy in Public Places



3.33 Robert Post has suggested that the underlying structure of the US tort of privacy serves to promote rules of behaviour and civility in society.[81] Solove contends this means that privacy, which is usually viewed as an individual's effort to keep the rest of society at bay, is itself an expression of society's will:

> *Privacy is not simply a way to extricate individuals from social control, as it is itself a form of social control that emerges from society's norms. It is not an external restraint on society, but is in fact an internal dimension of society. Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society.*[82]

DOES PRIVACY EXTEND TO PUBLIC PLACES?

THE TRADITIONAL VIEW

3.34 Traditionally, the view has been taken that there is no right to privacy in public places.[83] That 'traditional view' may no longer be supportable. Caoilfhionn Gallagher, for example, has noted that 'in medieval plays prying and eavesdropping, often took place indoors, and private, snatched, romantic moments took place outside, in gardens and on balconies.'[84] The Surveillance Studies Network notes that traditionally anonymity in public places was a means of escape from 'the intense human surveillance strictures of small communities'.[85] It may be that the notion of the home as a private space is a recent phenomenon for most people, due to smaller family size, affluence and relatively large homes.

3.35 In 1960, however, William Prosser rejected the notion that one had a right to privacy in a public place when describing the tort of intrusion, one of four privacy torts in the United States. He wrote:

> *On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about. Neither is it such an invasion to take his photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which any one present would be free to see.*[86]

3.36 In the United Kingdom, where the action for breach of confidence has long been available for some forms of privacy infringement, the courts held that it did not extend to events in public places. According to the courts, disclosure of information about events that took place in public did not have a quality of confidence about them.[87] For example, in *Woodward v Hutchins*, Lord Denning MR said that the disclosure of an incident in which a number of pop stars took drugs and behaved outrageously while on an airplane flight could not be disclosure of confidential information 'because the band members were in a publicly accessible place when the events took place'.[88]

3.37 In Canada, the courts have been similarly reticent to extend general law privacy protection to public places.[89] One court, for example, dismissed an action for invasion of privacy by a woman whose friend had circulated a photograph of her taken on holiday when she was topless. According to the court, the fact that the photograph had been seen by a photograph developer in Hawaii meant that she no longer had an expectation of privacy in relation to the defendant's friends to whom the photograph had been circulated.[90]

3.38 According to Elizabeth Paton-Simpson, the traditional view has been that people have a responsibility upon entering a public place to shield private information. Failure to do so waives their right to privacy.[91] Paton-Simpson refers to this as the law's insistence that we act as 'paranoids' while in public places. As an example, she quotes the Younger Committee in Britain which in 1972 advised against the creation of a legal right to privacy favouring instead:

> *guarded speech about one's personal affairs, care of personal papers, caution in disclosing information on request, confining private conduct to secluded places, and the use of curtains, shutters and frosted glass.*[92]

A MODERN VIEW: PRIVACY FOLLOWS THE PERSON

3.39 The strict view that privacy ends when we leave our homes does not enjoy universal support. A key development was the 1967 United States Supreme Court decision *Katz v United States*.[93] In that case the Supreme Court found a violation of the US Constitution's Fourth Amendment prohibition on searches without a warrant when the government monitored a telephone conversation occurring in a public phone booth.[94] In doing so, the court rejected the notion that the privacy protected by the Fourth Amendment was dependent on place:

> *the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection…But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.*[95]

The court articulated a test for privacy based on a person's reasonable expectation. Justice Harlan's referred to a twofold requirement, 'first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable".'[96]

3.40 While *Katz* signalled that being in a public place would no longer be an absolute bar to privacy protection, as the discussion below will show, courts in the United States and other places, such as New Zealand and Hong Kong, have been reluctant to find that people have a reasonable expectation of privacy in public places. Fourth Amendment cases decided after *Katz* have generally found it unreasonable to expect privacy in activities exposed to public view.[97]

3.41 Further, the US tort of privacy, which also relies on the reasonable expectation of privacy test, has limited application in public places.[98] A recent review of case law[99] found examples of surveillance practices that were deemed not to invade privacy including: 'a private investigator's surveillance from a public street of a person outside his home';[100] 'tracking of the daily commute of a school principal suspected of living outside the city in violation of residency requirements';[101] and 'photographing and publishing of a picture of persons in public seating at a racetrack'.[102]

81 Ibid 762-763 citing Robert C Post, 'The Social Foundations of Privacy: Community and Self in the Common Law' (1989) 77 *California Law Review* 957, 968

82 Ibid 763.

83 See eg, William Prosser, 'Privacy' (1960) 48 (3) *California Law Review* 383, 391-392.

84 Caoilfhionn Gallagher, 'CCTV and Human Rights: The Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41' (2004) 2 (2/3) *Surveillance & Society* 270, 279.

85 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [11.2.1].

86 William Prosser, 'Privacy' (1960) 48 (3) *California Law Review* 383, 391-392.

87 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 611-612.

88 Woodward v Hutchins [1977] 1WLR 760, 764 cited in Ibid 613.

89 See, eg, Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 318; and Sjaak Nouwt, Berend R de Vries, Roel Loermans, 'Analysis of the Country Reports' in Sjaak Nouwt, et al (eds) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (2005) 323, 333.

90 *Milton v Savinkoff* (1993) 18 CCLT (2d) 288 (BCSC) cited in Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 315.

91 Ibid 308, 320.

92 Ibid 307 quoting *Report of the Committee on Privacy* [UK] (1972) (Chair: K Younger) 25.

93 389 US 347 (1967).

94 *Katz v United States*, 389 US 347, 351-352 (1967).

95 *Katz v United States*, 389 US 347, 351 (1967).

96 *Katz v United States*, 389 US 347, 361 (1967).

97 See, eg, *United States v Knotts*, 460 US 276 (1983) which held that the government can track a criminal suspect's car using a beeper and without a warrant, because one does not have a reasonable expectation of privacy when driving in a public road.

98 Camrin Crisci, 'All the World is Not a Stage: Finding a Rights to Privacy in Existing and Proposed Legislation' (2002) 6 *Legislation and Public Policy* 207, 228 citing Andrew Jay McClurg, 'Bringing Privacy Law Out of the Closet: a Tort Theory of Liability for Intrusions in Public Places (1995) 73 *North Carolina Law Review* 989, 1086-87. Paton-Simpson has written that this has led to some striking decisions in the United States where privacy claims have not been recognised, including for an individual photographed standing in an unemployment queue, people entering an abortion clinic, attendees at a union meeting, and an individual engaged in sexual activity in a parking lot. Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 311-313.

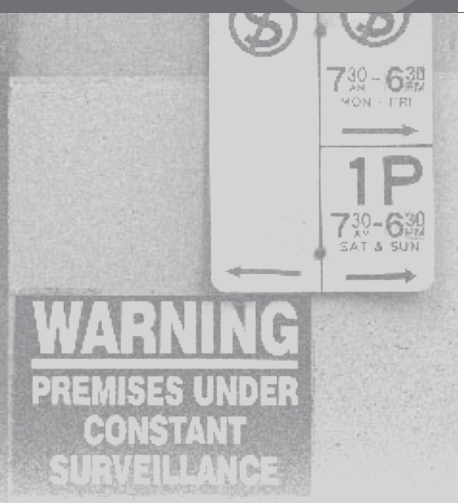
99 Deckle McLean, 'Plain View: A Concept Useful to the Public Disclosure and Intrusion Privacy Invasions Torts' (1999) 21 *Communication and the Law* 9.

100 Ibid 10 citing *Johnson v Corporate Special Services,* 602 So. 2d 385 (Ala, 1992).

101 Ibid 13 citing *Munson v. Milwaukee Board of School Directors*, 969 F 2d 266 (7th Cir 1992).

102 Ibid citing *Schifano v. Green County Greyhound Park,* 624 So 2d 178 (Ala,1993).

Chapter 3 Privacy in Public Places



3.42 In New Zealand, it appears unlikely that the recently recognised tort of invasion of privacy extends to public places. In *Hosking v Runting* the Court of Appeal of New Zealand held that children of a celebrity did not have their privacy breached when the media photographed them in a public place.[103] The court said:

> *The inclusion of the photographs of Ruby and Bella in an article in* New Idea! *would not publicise any fact in respect of which there could be a reasonable expectation of privacy. The photographs taken by the first respondent do not disclose anything more than could have been observed by any member of the public in Newmarket on that particular day.*

3.43 By contrast, the European Court of Human Rights has extended privacy protection to public places. In *PG and JH v United Kingdom*, the Court concluded that covert recordings of suspects at a police station (not traditionally viewed as a private place) interfered with their right to privacy on the basis that there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"' as the term is used in Article 8 of the Convention'.[104]

3.44 In *Peck v United Kingdom* the Court found a violation of Article 8 in a local council's failure to take precautions (such as masking images and obtaining consent) before releasing CCTV footage of a man attempting suicide while on a public street to the media.[105] In *Von Hannover v Germany* the court found a violation of Article 8 in the publication of photographs of Princess Caroline of Monaco doing no more than 'engaging in sport, out walking, leaving a restaurant or on holiday'.[106]

3.45 It has been observed that the decision in *Von Hannover* is essentially an application of French privacy law.[107] In France, the publication of a person's photograph taken in a public place is illegal unless the person's image is incidental in the photograph.[108] Thus,

> *Where the complaining person is the main subject [of a photograph]…he can object to the publication on the ground of privacy…The person is not, however, entitled to do so where his image is only one of the component elements of a whole public subject, even though he may still be identifiable.*[109]

3.46 The Canadian Supreme Court considered a similar law in the province of Quebec in *Aubry v Éditions Vice-Versa Inc* finding that media publication of an image of a person sitting on the steps of a building was a breach of that person's privacy.[110] The court found the right to one's image to be part of the right to privacy under the Quebec Charter.[111]

3.47 The reasonable expectation of privacy test also exists in the UK.[112] Until recently, its application in public places was neither as broad as the European Court nor as restrictive as in the United States.[113] The leading case is *Campbell v Mirror Group Newspapers Ltd*[114] where the House of Lords held that a newspaper had infringed model Naomi Campbell's right to privacy when it published a photograph of her leaving a Narcotics Anonymous meeting. On one view, it was the private nature of the activity, dealing with an intimate or personal act (treatment for drug addiction), that was protected and were she photographed doing nothing more than going about her business in public the claim may not have succeeded.[115]

3.48 In the more recent case of *Murray v Big Pictures (UK) Ltd* (the J.K. Rowling Case),[116] which concerned publication of a photograph of the child of writer J.K. Rowling taken in a public street, the Court of Appeal concluded that there was a reasonable expectation of privacy in the circumstances despite the fact that there was no intimate or personal activity involved. According to the Court, a number of factors, such as the covert and planned nature of the photography, as well as lack of consent, made the conduct unlawful.

OTHER EVIDENCE OF A REASONABLE EXPECTATION OF PRIVACY IN PUBLIC PLACES

3.49 From their behaviour, most people demonstrate an expectation of some privacy when in public places. Examples include wearing clothing to hide intimate areas of the body and avoiding discussion of personal matters when there is a reasonable expectation of being overheard.[117] Most people also follow various social conventions in public places to limit interference with the privacy of others.[118] Examples include conventions about personal space, such as how close to stand to others, and limits on staring at other people.[119]

3.50 During initial consultations, the commission was told by several groups that people have an expectation of privacy in many outdoor areas, as well as publicly accessible indoor areas.[120] One young person suggested that while it may be unreasonable to expect to be *invisible* in public, it is not unreasonable to expect some privacy.[121] On the other hand, many surveillance user groups felt that privacy does not extend to public places,[122] and some noted that the only truly private place is a person's home.[123] In our consultations with the media, some participants suggested that the media are entitled to record any image in a public place,[124] and one view was that this even extends to private conversations in public places.[125]

3.51 Some members of the Victorian parliament acknowledged the expectation of privacy in some public places, such as the beach, when considering the *Surveillance Devices Act* (SDA (Vic)) in 1999.[126] For example, the former Victorian member for Knox Mr Hurtle Lupton said:

> *Although beaches are very public places, people are entitled to have their right to privacy respected when they walk along them. If people are videoed while engaging in such activities and those videos are broadcast, irreparable damage could be caused. I acknowledge that it would be difficult to introduce legislation to prohibit or prevent such surveillance.*[127]

3.52 The European Commission's Data Protection Working Party[128] emphasised the privacy expectation of people in public places when considering the impact of surveillance:

> *A considerable portion of the information collected by means of video surveillance concerns identified and/or identifiable persons, who have been filmed as they moved in public and/or publicly accessible*

103 *Hosking v Runting* [2003] 3 NZLR 285.

104 *PG and JH v United Kingdom* (2001) IX Eur Court HR [56]-[57] [emphasis added]. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 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 in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.'

105 *Peck v United Kingdom* (2003) I Eur Court HR [80].

106 *Von Hannover v Germany* (2004) III Eur Court HR 294 [61], [80].

107 Yan Mei Ning, 'Media Photography in Hong Kong Streets: The Impact of Proposed Privacy Torts' (2006) 11 (2) *Media and Arts Law Review* 161, 186 citing Duncan Lamont, 'Is This the End of the Paparazzi?', *Guardian* (London), 28 June 2004, 6.

108 Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy,* Report (2004) 191 citing Étienne Picard, 'The Right to Privacy in French Law' in Basil S Markesinis (ed) *Protecting Privacy* (1999) 90 and 95.

109 Étienne Picard, 'The Right to Privacy in French Law' in Basil S Markesinis (ed) *Protecting Privacy* (1999) 90.

110 *Aubry v Éditions Vice-Versa Inc* [1998] 1 SCR 591.

111 *Aubry v Éditions Vice-Versa Inc* [1998] 1 SCR 591 [51].

112 However, this is in respect of proceedings for breach of confidence not any tort of invasion of privacy. The Law Reform Commission of Ireland has similarly adopted the view of privacy in public, saying: 'Since we view privacy as a personal right and one that follows the personal space of the person it follows that a "reasonable expectation" of privacy may even exist in public places.' Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [2.11].

113 Referring to the action for 'breach of confidence' which in England is forming the basis for a privacy tort, Lord Nicholls in *Campbell v MGN Ltd* [2004] 2 AC 457, [21] described the test of whether or not something is private as depending on 'whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy'.

114 [2004] 2 AC 457

115 Gavin Phillipson, 'Privacy in England and Strasbourg Compared' in Andrew Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 184, 204 and 207-208 quoting Baroness Hale in *Campbell v MGN Ltd* [2004] 2 AC 457 [24]: 'If this had been, and had been presented as, a picture of Naomi Campbell going about her business in a public street, there could have been no complaint…'.

116 [2008] EWCA Civ 446.

117 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 618.

118 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 326.

119 Ibid 326.

120 Roundtables 16 and 17.

121 Roundtable 22.

122 Roundtables 1, 4, 12, 19, 31,

123 Roundtables 19 and 31.

124 Roundtable 27.

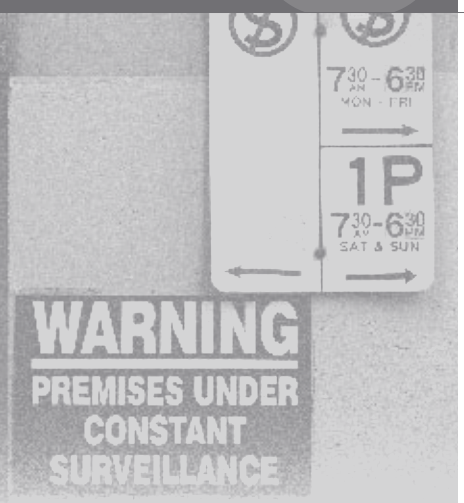
125 Roundtable 27.

126 Victoria, *Parliamentary Debates,* Legislative Council, 11 May 1999, 524–525 (Maree Luckins); Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 551 (Robert Hulls), 555 (Victor Perton), 559 (Hurtle Lupton).

127 Victoria, *Parliamentary Debates,* Legislative Assembly, 22 April 1999, 559 (Hurtle Lupton).

128 An independent advisory body on data protection and privacy: Article 29 Data Protection Working Party, European Commission, *Working Document on the Processing of Personal Data by Means of Video Surveillance* Adopted on 25 November 2002:11750/02/EN: WP 67 (2002) 1 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf> at 9 January 2009.

Chapter 3 Privacy in Public Places



premises. Such an individual in transit may well expect a lesser degree of privacy, but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image.[129]

FACTORS RELEVANT TO THE EXPECTATION OF PRIVACY IN PUBLIC

3.53 While there may be shared expectations of privacy in public places, the extent and reasonableness of those expectations will differ according to context. Commentators have identified a number of factors relevant to the expectation of privacy in public places.[130] They include location, the intimate or sensitive nature of the activity, the making of a record and dissemination, the form of surveillance, whether or not the person under surveillance is a public figure, whether surveillance focused on a person or was harassing in nature, use of technology, the covert nature of the surveillance, and consent.[131] N.A. Moreham suggests that at least two of these factors should exist in order to claim a reasonable expectation of privacy in a public place.[132]

LOCATION

3.54 The first factor to be considered when assessing whether there is a reasonable expectation of privacy in a public place is the location of the activity. The term 'public place' covers a variety of settings, ranging from 'bustling thoroughfares to remote getaways',[133] where expectations of privacy may differ quite substantially. Also, as Paton-Simpson notes, the distinction between a public place and private place is one of degree.[134]

3.55 Moreham suggests that expectations of privacy in public places depend on two characteristics: 1) the numbers of people a person is exposed to; and 2) the nature of the people that a person is exposed to.[135] With respect to numbers, there is a greater expectation of privacy in locations containing few people, such as a quiet park, than locations where you may exposed to many, for example in a crowded shopping centre.

3.56 When surrounded by fewer people, most of us are more likely to let down our guard and less likely to make an effort to conceal private information. According to Moreham, 'people quite reasonably adapt their self-presentation efforts according to their assessment of who can observe them and will usually have fewer inhibitions and make fewer self-presentation efforts when fewer people are around'.[136] Similarly, Paton-Simpson says that '[r]easonable people assess roughly just how "public" a situation is and adjust their behaviour accordingly.'[137]

3.57 Both users of public place surveillance and community groups suggested during consultations that expectations of privacy are greater in some locations than others. For example, we learned that one government-run insurer considers reasonable expectations in determining whether to conduct surveillance and, as a result, avoids surveillance in areas such as swimming pools, court precincts, funerals, weddings and change rooms.[138] In both the local government/police and private investigator roundtables, the commission was told there is a public perception that backyards may be locations where people should not be subjected to surveillance, particularly when they are not easily observed from a public place.[139] A number of groups suggested that 'no go' areas for surveillance include toilets and change rooms.[140]

INTIMATE OR SENSITIVE NATURE OF THE ACTIVITY OR CONVERSATION

3.58 A second factor to be considered when assessing whether there is a reasonable expectation of privacy in a public place is the nature of the activity concerned: whether a person is engaged in a 'particularly intimate, traumatic or humiliating' matter[141], for example, attending a funeral. The Law Reform Commission of Ireland notes that there is a greater expectation of privacy from surveillance 'at a time of death, injury or grieving, where those affected are vulnerable or are otherwise unable at the time to fend off such surveillance'.[142]

3.59 A number of court decisions demonstrate the significance of the nature of the activity in question when considering whether there is a reasonable expectation of privacy. For example, until recently, UK law did not extend privacy protection to public places unless the activity was of an intimate or private nature, such as leaving an abortion clinic.[143] As we noted earlier, the recent J.K. Rowling case appears to have extended privacy protection

by finding a reasonable expectation of privacy in a public place.[144] In that case factors such as the lack of consent, the covert and planned nature of the photography, and the fact that the claimant was a child, raised the expectation of privacy.

3.60 In *Hosking v Runting*, the New Zealand Court of Appeal acknowledged that while 'generally there is no right to privacy when a person is photographed on a public street', there may be exceptional cases where 'a person might be entitled to restrain additional publicity being given to the fact that they were present on the street in particular circumstances'.[145]

3.61 The expectation of privacy may also be greater when the intimate activity in question is involuntary. For example, a court in the United States held a newspaper liable for publishing a photograph of a woman whose skirt had, through no fault of her own, blown up at a 'Fun House'.[146] The embarrassing scene, the court said, was beyond her control.

3.62 By contrast, a person who purposefully engages in an activity likely to attract public attention may be less entitled to claim a reasonable expectation of privacy.[147] In *Friedl v Austria*, the European Court of Human Rights concluded that there had been no violation of Article 8 when a photograph was taken of an individual at a public demonstration, in part because the person had chosen to participate in that activity.[148]

MAKING A RECORD AND DISSEMINATION

3.63 Whether public place surveillance activity leads to the creation of a permanent record and whether that record is widely shared may be relevant when considering if there is a reasonable expectation of privacy.

3.64 Mere monitoring of a public place by a surveillance device may not generate a reasonable expectation of privacy for reasons explained by the European Court of Human Rights in *PG and JH v United Kingdom*:

> *A person who walks down the street, will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.*[149]

129 Article 29 Data Protection Working Party, European Commission, *Working Document on the Processing of Personal Data by Means of Video Surveillance* Adopted on 25 November 2002:11750/02/EN: WP 67 (2002) 5 <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf> at 9 January 2009..

130 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998)[2.13]-[2.19] noting that their list of factors is not exhaustive.

131 Ibid

132 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 620.

133 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 321.

134 Ibid 322.

135 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 622-623.

136 Ibid 622.

137 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 322.

138 Roundtable 2.

139 For example where hedges, fences or other structures prevent visual observation: Roundtables 8 and 25.

140 Roundtables 2, 8, 9, 10, 12, 13, 14, 15, 20, 21, 24, 25, 26, 27. Note also that this view is in line with the Explanatory Memorandum, Surveillance Devices Bill 1999 (Vic) cl 3.

141 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 623.

142 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [2.14].

143 Gavin Phillipson, 'Privacy in England and Strasbourg Compared' in Andrew Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 184, 204.

144 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.

145 *Hosking v Runting* [2003] 3 NZLR 285 [164] [emphasis added].

146 *Daily Times Democrat v Graham* (1964) 162 So 2d 474, 476-478.

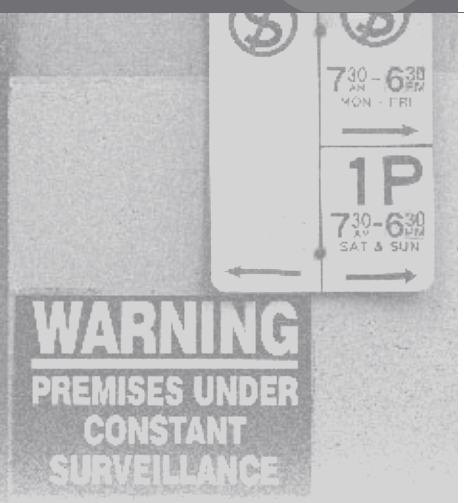
147 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 627.

148 *PG and JH v United Kingdom* (2001) IX Eur Court HR [58] discussing *Friedl v Austria* (1994) 31 Eur Comm HR [51]-[52].

149 *PG and JH v United Kingdom* (2001) IX Eur Court HR [57].

Chapter 3

Privacy in Public Places



3.65 Similarly, the European Commission for Democracy Through Law Reform (the Venice Commission), the Council of Europe's advisory body on constitutional matters,[150] has contrasted the privacy expectation in mere monitoring with the expectation when a record is made:

> *it is not the monitoring as such which is the most problematic, but the recording of the data and their processing which may create an unlawful interference with the right to privacy, especially if the data have been collected by covert surveillance methods.*[151]

3.66 In part, the different privacy expectation with respect to a mere observation and a permanent record is due to the power of the photographic image. Both the European Court of Human Rights[152] and the UK Court of Appeal have discussed the special place of photographs.[153] Thus, in *Douglas v Hello! Ltd (No 3)*, the UK Court of Appeal said about photographs:

> *They are not merely a method of conveying information that is an alternative to verbal description. They enable the person viewing the photograph to act as a spectator, in some circumstances voyeur would be the more appropriate noun, of whatever it is that the photograph depicts. As a means of invading privacy, a photograph is particularly intrusive.*[154]

3.67 The heightened expectations of privacy when there is a permanent record is reflected in information privacy laws which generally require the creation of a record before privacy protection applies.[155] This sentiment was expressed in consultations with community groups, when we were told that while people must expect to be seen by others when engaged in recreational activities in public (such as being in the park with kids, or sitting on the beach), people do not expect to have their photograph taken with another person's mobile phone when doing these things.[156]

3.68 Andrew McClurg has suggested that a photograph intensifies an invasion of privacy in three ways.[157] First, it allows the photographer to take a part of the subject with him or her converting an otherwise temporary experience into a prolonged act.[158] Indeed, the temporary or fleeting nature of our actions in public is, according to Jeffrey Reimen, a form of privacy protection because 'privacy results not only from locked doors and closed curtains but also from the way our publicly observable activities are dispersed over space and time'.[159] But, 'a photograph…allows the scrutiny to be extended indefinitely'.[160]

3.69 The second way in which a photograph intensifies the privacy invasion is that it may reveal information that a temporary observation with the naked eye would not disclose[161] because it provides the time needed to 'detect subtleties'.[162]

3.70 Third, a photograph may multiply the privacy invasion through its dissemination.[163] Dissemination results in a differently constituted, and possibly broader, group of people having access to personal information without consent.[164] For example, a topless sunbather has agreed to allow a limited group of observers to see her incidentally on the beach, but she has not consented to observation by the infinitely larger audience on the internet should photographs of her be posted there.[165]

3.71 Dissemination also takes control over access to personal information from the surveillance subject and places it with the surveillance user: 'if X obtains the photograph of Y then he, and not just Y, will be able to determine who gets to see her naked body.'[166]

3.72 In some jurisdictions, dissemination must occur before the law provides any privacy protection. For example, in the UK it appears that taking a photograph on a public street is not in itself a breach of privacy. In *Campbell*, Lord Hope said: 'the taking of photographs in a public street must…be taken to be one of the ordinary incidents of living in a free community.'[167] Lord Hoffman said: 'the famous and even the not so famous who go out in public must accept that they may be photographed without their consent, just as they may be observed by others without their consent'.[168] His Lordship went on to remark that 'the fact that we cannot avoid being photographed does not mean that anyone who takes or obtains such photographs can publish them to the world at large'.[169]

FORM OF SURVEILLANCE

3.73 Expectations of privacy may be greater when particular forms of surveillance are used. For example, people may have greater expectations of privacy in relation to their conversations in public places than with respect to their images. Similarly, people may have a heightened expectation of privacy with respect to information gathered through tracking surveillance, as it can give the surveillance user information about where they have been, who they have been with, and what activities they have engaged in.

3.74 The view that surveillance of aural communications heightens expectations of privacy was expressed in our consultations. In a media roundtable it was suggested that while a person would not expect a whisper in a friend's ear to be subject to surveillance, people must expect to be seen when in a public place.[170] Similarly, it was noted at the roundtable involving financial service providers that while a person should expect visual surveillance in a bank, audio surveillance is not used partly out of respect for the privacy of conversations between customers and tellers.[171]

WHETHER OR NOT THE PERSON UNDER SURVEILLANCE IS A PUBLIC FIGURE

3.75 Whether a person is a public figure may affect the reasonableness of any expectation of privacy while in public. Public figures, such as members of parliament and celebrities, may reasonably expect less privacy than others, particularly regarding activities that relate to their public functions. This view found support in our consultations with the media.[172]

3.76 Nevertheless, there is a view that public figures maintain some level of privacy in public, especially in relation to intimate and private activities.[173] In *Von Hannover v Germany*,[174] the European Court of Human Rights went further by protecting the right to privacy of a public figure (Princess Caroline of Monaco) with respect to everyday activities conducted in public, including leaving a restaurant and practising sport.[175]

FOCUSSING UPON ON A PERSON OR ENGAGING IN HARASSMENT

3.77 Reasonable expectations of privacy may increase when surveillance is focussed on a particular individual, rather than an indeterminate group of people. For example, in *Aubry v Editions* the Canadian Supreme Court noted that where a person's image appears incidentally in a photograph taken in a public place, the public interest in the publication of the photograph prevails over the

150 *Presentation*, Council of Europe, Venice Commission, <www.venice.coe.int/site/main/presentation_E.asp?MenuL=E> at 2 December 2008.

151 European Commission for Democracy for Law (Venice Commission), *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights* study no 404 (2007) [29] citing *Amann v Switzerland* (2000) II Eur Court HR [65]-[66].

152 *Von Hannover v Germany* (2004) III Eur Court HR 294.

153 *Mosley v New Group Newspapers Ltd* [2008] EWHC 1777 (QB) [18]-[19].

154 [2006] QB 125 [84].

155 British Institute of International & Comparative Law, *The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data* Report (Service Contract CNS/2002/AO-7002/A/55) 61-62.

156 Roundtable 17.

157 Andrew McClurg, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places' (1995) 73 *North Carolina Law Review* 989, 1041.

158 Ibid 1041-1042.

159 Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Computer and High Technology Law Journal* 27, 29.

160 Andrew McClurg, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places' (1995) 73 *North Carolina Law Review* 989, 1042.

161 Ibid 1042.

162 Ibid 1042.

163 Ibid 1042.

164 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 618.

165 Ibid 614.

166 Ibid 634 quoting Andrew McClurg, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places' (1995) 73 *North Carolina Law Review* 989,1041-1042.

167 *Campbell v MGN Ltd* [2004] 2 AC 457 [122].

168 *Campbell v MGN Ltd* [2004] 2 AC 457 [73].

169 *Campbell v MGN Ltd* [2004] 2 AC 457 [74].

170 Roundtable 26.

171 Roundtable 29.

172 Roundtable 26.

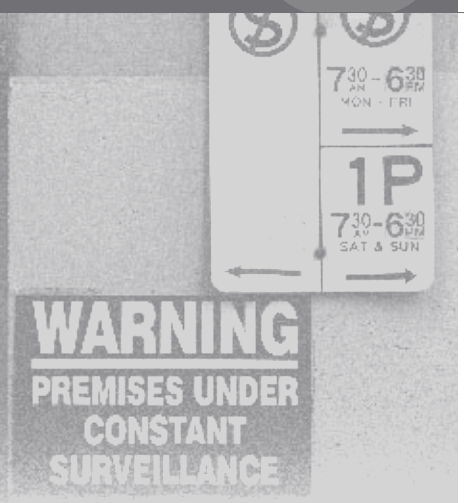
173 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [2.17].

174 *Von Hannover v Germany* (2004) III Eur Court HR 294.

175 *Von Hannover v Germany* (2004) III Eur Court HR 294 [61].

Chapter 3

Privacy in Public Places



right to privacy of the incidental subject.[176] The court noted that in such a situation 'the unforseen observer's attention will normally be directed elsewhere' in the photograph and 'the person "snapped without warning" cannot complain'.[177]

3.78 The expectation of privacy in public places may also be greater where surveillance is persistent or harassing rather than isolated or incidental. The Law Reform Commission of Ireland has suggested that while casual photography in a public place would not normally be deemed an invasion of another's privacy, 'targeting of a particular individual either surreptitiously or against his or her will in a public place', and 'deliberate following (whether surreptitious or otherwise) of a person from place to place with a view to observing his or her movements' could be an invasion of privacy.[178]

3.79 Harassment and persistent surveillance is particularly problematic because it can produce a detailed picture of a person's life which can subsequently be used by others to draw conclusions (whether right or wrong) about that person.[179]

3.80 A number of court decisions in different jurisdictions have been influenced by the harassing nature of the surveillance in question. For example, it appears that the harassing nature of the public place surveillance to which Princess Caroline of Monaco was subjected by a member of the paparazzi was critical to the European Court of Human Right's decision that this behaviour amounted to a breach of privacy.[180] Similarly, in the United States an exception to the common law's refusal to find privacy rights in public places occurs where monitoring of a person in public has amounted to harassment and hounding.[181] In *Gallela v Onassis*, a court granted relief to Jacqueline Onassis against a paparazzo who had engaged in a course of conduct, including surveillance of her children and their school and using bribes to gain access to private locations.[182]

3.81 In our roundtable consultations with government, sport and entertainment bodies it was suggested that there would be a reasonable expectation of privacy with respect to CCTV if it was used to focus on an individual for an extended length of time and used to follow a person for no proper purpose.[183]

USE OF TECHNOLOGY AND COVERT NATURE

3.82 It is arguable that there is a heightened expectation of privacy when surveillance occurs not merely with the naked eye, but by using technology that can enhance observation and which may be unseen. As noted in Chapter 2, rapid developments in technologies have created 'limitless potential to contravene normal expectations of privacy in both public and private places'.[184] Modern surveillance technologies can observe activities at great distance, can see through walls, and even through clothes.[185]

3.83 Technology now transcends the physical barriers that once afforded people a degree of privacy in public places. Paton-Simpson notes that 'in the ordinary course of things, a person expects to be observed only from certain angles and distances and does not expect to be scrutinised in close-up without realizing and being able to react.'[186] Moreham also comments on the changes brought about by the ability of new technology to pierce 'self-presentation barriers':

> *Few would dispute, for example, that Y, who wears clothes to avoid revealing her body in public, would have a reasonable expectation that Z would not use an x-ray device to see through her clothing or…that X and Y would have a reasonable expectation that Z would not record their conversations with a shotgun microphone.*[187]

3.84 New information technologies also have the ability to amass and link significant amounts of information about our public activities.[188] The implications of gathering or 'assembling' information are that:

> *by accumulating a lot of disparate pieces of public information, you can construct a fairly detailed picture of a person's private life. You can find out who her friends are, what she does for fun or profit, and from such facts others can be inferred, whether she is punctual, whether she is faithful, and so on.*[189]

3.85 Technological advances have also lead to smaller and more covert forms of surveillance.[190] Covert surveillance is a matter of concern because a person has no opportunity to alter their behaviour to avoid revealing private information. For example, if most people knew they were being monitored by a powerful microphone when sitting on a park bench they would stop discussing an intimate subject. Similarly, if a sunbather knew her photograph was being taken to be placed on the internet, she may decide to cover herself or move to another location.[191]

3.86 This point was made in the English case, *R v Broadcasting Standards Commission ex parte British Broadcasting Corp*, where the Court of Appeal said that secret filming denies the person filmed an opportunity to refuse consent, or to take measures to ensure their activity is not filmed.[192] The covert nature of surveillance was also a relevant factor in *Murray v Big Pictures (UK) Ltd* where Clarke MR concluded that the fact that the photograph of J.K. Rowling's child 'was taken covertly by a photographer using a long range lens' was a relevant factor when considering the reasonable expectation of privacy.[193]

WHETHER CONSENT WAS GIVEN

3.87 People may not have a reasonable expectation of privacy if they have consented expressly or impliedly to an act of surveillance in a public place. An example of express consent is when an individual gives a newspaper photographer permission to take his or her photograph in public and to publish it.

3.88 Implied consent, which may be said to arise when a notice warns people entering an area that surveillance is taking place, is often more difficult to determine. This is because of the challenge in deciding whether the person had an effective choice to submit to the surveillance, or whether there was mere acquiescence rather than actual consent. [194]

3.89 Paton-Simpson argues that a person often has very little real choice about whether they subject themselves to surveillance because avoiding surveillance may mean refraining from very basic activities. According to Paton-Simpson, the 'choice', if there is one, is of 'taking a minor risk of public exposure or forgoing an activity or association altogether'.[195] For example, because many petrol stations are fitted with CCTV a person would have to give up driving a car to avoid this form of surveillance. Paton-Simpson also refers to the fact that if facial recognition technology is used in conjunction with CCTV at large events, 'the only sure way to avoid being detected arriving at a controversial gathering is not to attend.'[196]

176 *Aubry v Éditions Vice-Versa Inc* [1998] 1 SCR 591 [59].

177 *Aubry v Éditions Vice-Versa Inc* [1998] 1 SCR 591 [59].

178 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [2.13].

179 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 324.

180 Gavin Phillipson, 'The "Right" of Privacy in England and Strasbourg Compared' in Andrew Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 184, 210-211.

181 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 324.

182 *Gallela v Onassis*, 487 F 2d 986 (2nd Cir 1973). See also *Nader v General Motors Corp*, 255 NE 2d 765 (NY 1970).

183 Roundtable 4.

184 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 330.

185 See Bruce Phillips, 'Privacy in a "Surveillance Society"' (1997) 46 *University of New Brunswick Law Journal* 127, 129 in Ibid 330.

186 Ibid 330.

187 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 630.

188 Alpert in Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 324.

189 Reiman cited in Helen Nissenbaum, 'Protecting Privacy In An Information Age: The Problem of Privacy in Public' (1998) 17 *Law and Philosophy* 559, 589.

190 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 330.

191 N A Moreham, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606, 619.

192 *R v Broadcasting Standards Commission ex parte British Broadcasting Corp* [2000] EWCA Civ 116 cited in Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 331.

193 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446 [6] (Clarke MR).

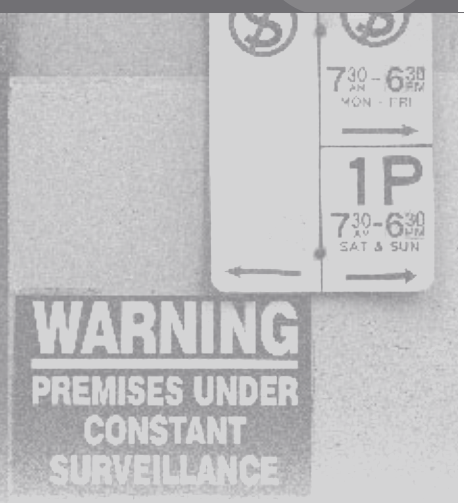
194 The Law Reform Commission of Ireland gives an example of implied consent (and not necessarily in the context only of public places) of people who have deliberately courted media publicity with respect to an aspect of their intimate lives. Such people 'cannot expect to be able to "switch off" at will the media or other attention which they have sought'. Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [2.18]

195 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 338.

196 Ibid.

Chapter 3

Privacy in Public Places



3.90 In addition, it has been suggested that we often overlook the fact that 'consent may be conditional or restricted in its scope'.[197] For example, we may be able to imply consent to being filmed as part of a crowd in a sports arena, but not to having our individual conversations recorded and broadcast to the whole stadium. Mere attendance at a stadium does not provide implied consent to all forms of privacy intrusion that might occur there.

PROTECTING 'PUBLIC PRIVACY' BEYOND REASONABLE EXPECTATIONS?

3.91 Persistent exposure to technology may cause attitudes to privacy to change because people feel that they have no choice. For instance, the growing prevalence of surveillance practices in public places may reduce expectations of privacy in public over time as people come to accept these practices.[198] Consequently, relying on a reasonable expectation of privacy test may not ensure adequate protection of public privacy in the future because what is 'reasonable' may depend upon the extent to which surveillance devices are used.

3.92 The main legislation governing surveillance practices, the SDA (Vic), relies, in part, on a version of the reasonable expectation of privacy test. It protects some activities from surveillance only if the parties 'ought reasonably to expect' that they will not be observed or overhead by another person.[199] In the future, if there are powerful listening devices operating throughout public places, it may no longer be reasonable for people to expect that a hushed conversation will not be overheard. In these circumstances, what is 'reasonable' would be determined by the capacity of the technology.

3.93 To prevent advances in technology driving the legal protection of privacy, some commentators have argued that privacy safeguards should be normative.[200] They suggest we ought to come to a shared view on what is the preferred level of privacy in public places, rather than allow attitudes towards privacy to fluctuate based on technological advances. David Anderson writes that such an approach is more in keeping with one of the identified purposes of privacy law, which is to preserve norms of civility. Anderson suggests that privacy:

> *is a means by which society defines its relationship with the individual, just as the law of battery or the laws of property do. The law says up to a point I am public property and others can touch me or enjoy my land or satisfy their curiosity about my life, but beyond that point I am autonomous and I have a right to control others' use of me.*[201]

3.94 The great challenge is to formulate a shared view of an appropriate level of privacy protection in public places. A number of points should be kept in mind when undertaking this exercise:

- When we protect public privacy we are protecting a broader notion of privacy. As Paton-Stimson has argued, 'a great deal of the information we regard as private is revealed, either directly or indirectly, in a public place at some point.'[202] These include taking out a video, borrowing a book from the library, going shopping, and going out on a date.[203] Other private behaviours that occur in public include, showing grief and humiliation, and sharing intimate thoughts with a companion.[204]
- Privacy is important. The various concepts of privacy discussed in this chapter suggest that it is a notion that incorporates a number of important interests and values, including dignity, autonomy, preservation of individuality, and the formation of personal relationships. It has political, economic, sociological, and psychological benefits, and it promotes civility in society. Before we lose all sense of privacy when in public, we ought to consider whether the gains brought about by surveillance technologies advances outweigh that loss.
- Protecting public privacy is especially important for those people who spend a disproportionate amount of their lives in public places. For example, the commission learned that homeless people conduct many of their private activities in public places such as cafes, parks and public toilets.[205]

Young people are more likely to use public spaces because they do not incur a fee,[206] and in order to exercise their autonomy or demonstrate independence. People with limited economic means are more likely to spend time in public places, because they share smaller homes with more people.[207] By contrast, the affluent are more likely to live in larger homes where they can seek privacy—such as in large gardens or private land.

3.95 Indeed, some commentators have argued that if private acts are legally protected only when performed in private places, privacy becomes a right enjoyed largely by the wealthy. According to Benjamin Goold:

> *For many people, public spaces are important simply because they offer an alternative to the claustrophobic physical environments in which they spend the majority of their lives. For students in tiny, run-down apartments or families living in housing projects, for example, public parks and gardens can provide much needed space and room for recreation.*[208]

CONCLUSION

3.96 While difficult to define, privacy is a fundamental human right that encompasses many individual and societal values. It is now widely acknowledged that expectations of privacy extend to public places, although the reasonableness of any expectation will depend on the circumstances.

3.97 What is the impact of surveillance practices on privacy in public places? Are there other rights and interests at risk? How do we balance these risks against the benefits of public place surveillance? The next chapter explores these questions.

197 Ibid 334.

198 See eg, Caoilfhionn Gallagher, 'CCTV and Human Rights: The Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41' (2004) 2 (2/3) *Surveillance & Society* 270, 273; Anderson in Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 340; Aimee Jodoi Lum, 'Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Sphere' (2005) 27 *Hawaii Law Review* 377, 386.

199 *Surveillance Devices Act 1999* (Vic) 3.

200 See eg, David Anderson, 'Fundamental Issues in Privacy Law' in Basil Markesinis (ed) *The Clifford Chance Lectures: Volume 1: Bridging the Channel* (1996) 129.

201 Ibid 129.

202 Elizabeth Paton-Simpson, 'Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places' (2000) 50 (3) *University of Toronto Law Journal* 305, 340-341.

203 Ibid 341.

204 Nagle in Lisa Austin, 'Privacy and the Question of Technology' (2003) 22 (2) *Law and Philosophy* 119, 145–146.

205 Roundtable 16.

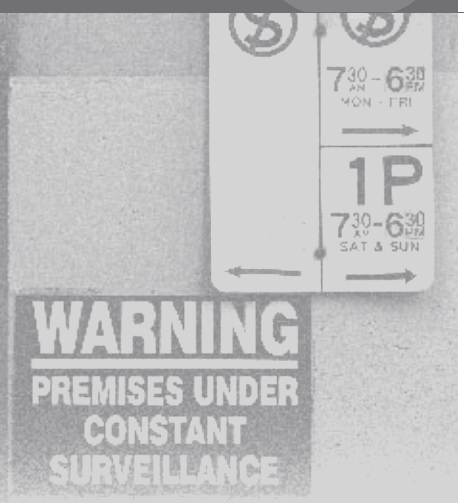
206 Roundtable 22.

207 Roundtable 16.

208 Benjamin Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance"' (2006) 25 (1) *Criminal Justice Ethics* 3, 5.

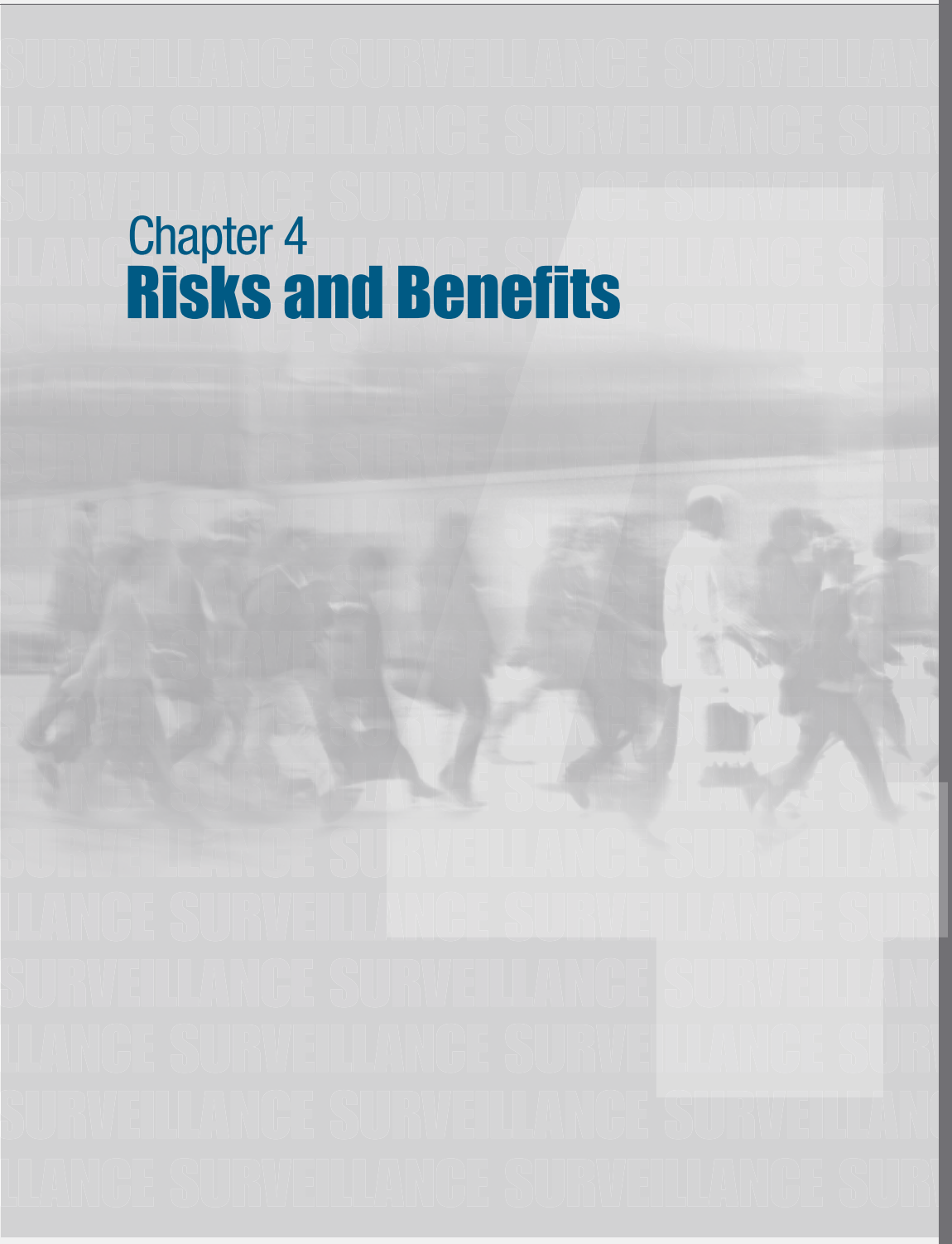
Chapter 3

Privacy in Public Places



Chapter 4

Risks and Benefits



Chapter4 Risks and Benefits

INTRODUCTION

4.1 In Chapter 2, we described the many ways in which Victorians experience surveillance in public places. Examples include the widespread presence of closed-circuit television (CCTV) on city streets and in shops, tracking surveillance in public transport, and the use of mobile phones as cameras. In this chapter, we consider the impact that surveillance may have on the lives of ordinary Victorians.

4.2 Many questions arise when considering the impact of public place surveillance. Is public place surveillance harmful if left unregulated because it is a threat to human rights, such as the right to privacy? Will the 'surveillance society'[1] irreversibly change the way we live because we will always feel that we are being watched when in public places?

4.3 On the other hand, is it right, as is commonly said, that 'if you've got nothing to hide, you've got nothing to fear'?[2] What are the benefits that flow from surveillance in public places? David Lyon has noted that we depend upon surveillance 'for the efficiency and convenience of many ordinary transactions and interactions'[3] How do we strike the proper balance to maximise the benefits and minimise the risks associated with public place surveillance?

CONCERN ABOUT PUBLIC PLACE SURVEILLANCE

4.4 Surveys suggest that the community generally supports the use of CCTV, which is one very prevalent form of public place surveillance. In a survey conducted for the Federal Privacy Commissioner in 2007, 79 per cent of respondents said they were not concerned about the use of CCTV in public places.[4] Similarly, a 2006 survey of Gold Coast residents and train commuters revealed a large majority supporting CCTV surveillance.[5] Many respondents, especially business respondents, stated that CCTV is not an invasion of privacy, nor a source of concern.[6] The prevailing view was 'anyone not happy [with CCTV] has something to hide'.[7] In the United Kingdom, an evaluation of CCTV systems in 2005 found broad support for CCTV[8] with only a small percentage of people believing the systems raise privacy concerns.[9]

4.5 The use of CCTV has proliferated recently. For example, in 2007 it was estimated that the UK, the world leader in CCTV use, had approximately 4.2 million cameras in operation.[10] Further, a survey in the capital cities of Austria, Denmark, Germany, Great Britain, Hungary, Norway and Spain found that one third of all premises and institutions operated CCTV cameras.[11] While similar data is not available in Australia, from our initial research and consultations the commission found that CCTV systems operate throughout the central business districts of most major cities.[12]

4.6 In the past decade, commentators have begun to raise concerns about the use of CCTV and other forms of public place surveillance. Simon Davies writes that in Britain early government and public support for CCTV ensured that 'the period up to 1996 was a difficult time for anyone wanting to challenge the rationale behind CCTV'.[13] However, in the mid-1990's things began to change, with academics, think tanks and other organisations questioning recourse to CCTV.[14] There was some direct action, including street theatre protests against CCTV[15] and a petition by 1,500 residents in the town of Hove in Britain opposing camera surveillance of their residential area.[16]

4.7 In 1995, the former Deputy Commissioner of the Metropolitan Police warned that Britain was becoming an Orwellian society where people were constantly under surveillance.[17] In October 1996, the surveillance watchdog organisation Privacy International issued a statement warning of 'a grave risk that the CCTV industry is out of control'.[18] In 2008, a British MP resigned from parliament and fought and won a subsequent by-election in order to highlight concerns about the erosion of freedoms, including the use of CCTV in public places.[19]

4.8 While survey research continues to show general support for CCTV in public places, Christopher Slobogin refers to a UK Home Office survey that reveals concerns about the practice.[20] While few people responded affirmatively when asked whether they had any concerns about CCTV cameras,[21] their responses to further questions are interesting:

- Seventy-two per cent agreed that cameras 'could easily be abused and used by the wrong people'
- Thirty-eight per cent agreed that the people in control of camera systems could not be 'completely trusted to use them only for the public good'
- Thirty-seven per cent felt that 'in the future, cameras will be used by government to control people'
- Eleven per cent agreed that 'these are really spy cameras and should be banned'.[22]

4.9 The previously mentioned European study found that despite general support for CCTV, 40 per cent of respondents agreed with the statement 'CCTV invades privacy' and 50 per cent agreed that 'CCTV footage can be easily misused'.[23] In addition, many respondents were sceptical about CCTV's effectiveness, with more than 50 per cent agreeing that 'CCTV displaces crime and does not protect against serious offences'.[24] The authors of the study also noted a lack of understanding of CCTV's actual functions and uses[25] with many people tending to overestimate the technological potential of the systems.[26] While most people were supportive of CCTV in banks and transport facilities, they were opposed to CCTV in intimate spaces such as change rooms.[27]

4.10 In Australia, the Federal Privacy Commissioner's 2007 study[28] noted greater unease among younger respondents, and among Victorians, as compared to the rest of the country.[29] Those people who expressed a concern about the use of CCTV in public places were likely to refer to the possibility of information being misused and/or the possibility of an invasion of privacy.[30] While 88 per cent of respondents supported access to CCTV footage by police, 'support for other organisations accessing footage [such as security companies, anti-terror organisations, and local councils] was considerably lower'.[31]

1 The expression 'surveillance society' emerged in the 1980s in studies of surveillance: Surveillance Studies Network, *A Report on the Surveillance Society* (2006), [3.5].

2 Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 748.

3 David Lyon, *Surveillance Society: Monitoring Everyday Life* (2001) 2.

4 Wallis Consulting Group Pty Ltd, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner* Reference No WG3322 (2007) 74.

5 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 46-47.

6 Ibid 49-50.

7 Ibid 49-50.

8 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 55.

9 Ibid 56. See also Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 8 on results from a European-wide survey published in 2004 which determined that a majority support CCTV (at 1) with two thirds of respondents agreeing with the statement 'who has nothing to hide, has nothing to fear from CCTV'.

10 Gareth Crossman et al, *Overlooked: Surveillance and Personal Privacy in Modern Britain* (2007) 2.

11 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 3.

12 See Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* A Report to the Criminology Research Council (CRC Grant 26/01-02) (2003) 24; and National Community Crime Prevention Programme in partnership with the Australian Institute of Criminology, *CCTV as a Crime Prevention Measure: What is CCTV?* Tip Sheet 5

13 Simon Davies, 'CCTV: A New Battleground for Privacy' in Clive Norris, et al (eds) *Surveillance, Closed Circuit Television and Social Control* (1998) 243, 244.

14 Ibid 243, 245.

15 Ibid 243, 249.

16 Ibid 243, 251.

17 Simon Davies, 'CCTV: A New Battleground for Privacy' in Clive Norris, et al (eds) *Surveillance, Closed Circuit Television and Social Control* (1998) 243, 245.

18 *Privacy International Statement on CCTV Surveillance*, Privacy International (15 October 1996) <www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61926> at 16 December 2008.

19 David Davis, 'David Davis's Statement in Full', *The Telegraph* (London), 12 June 2008 <www.telegraph.co.uk/news/newstopics/politics/conservative/2116741/David-Daviss-statement-in-full.html> at 21 January 2009.

20 Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 *Mississippi Law Journal* 213, 273.

21 Terry Honess and Elizabeth Charman, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness* (1992) 33.

22 Ibid 9.

23 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 8.

24 Ibid 9.

25 Ibid 1.

26 Ibid 8.

27 Ibid 8.

28 Wallis Consulting Group Pty Ltd, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner* Reference No WG3322 (2007) 74.

29 Ibid 74.

30 Ibid 75.

31 Ibid 76.

Chapter4 Risks and Benefits

4.11 Our own consultations with Victorian community and advocacy organisations in 2006 and 2007 revealed a number of concerns about public place surveillance. These included:

- who has access to surveillance footage[32]
- the effect of surveillance on political activity[33]
- use of surveillance footage to prosecute individuals, when the surveillance footage is of poor quality or before individuals have received legal advice[34]
- feelings of fear and intimidation experienced by young and Indigenous, people in relation to surveillance[35]
- exclusion of marginalised groups from public areas such as shopping centres[36]
- the effect on the society as a whole when its members are constantly watched.[37]

4.12 Concerns have also been raised about the impact of CityLink's payment system on anonymous travel in Victoria,[38] the potential of consumer products embedded with radio frequency identification (RFID) to invade the privacy of consumers by allowing businesses to track their movements long after they have left a store,[39] the potential voyeuristic use of the new x-ray body scanners at Melbourne airport,[40] and the privacy implications of internet search engine Google Street View.[41]

WHAT ARE THE RISKS ASSOCIATED WITH PUBLIC PLACE SURVEILLANCE?

4.13 Many of the risks associated with the abuse or overuse of public place surveillance are subtle and incremental. As Daniel Solove has noted, 'most privacy problems lack dead bodies'.[42] In many instances, according to Solove, 'privacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up'.[43]

4.14 In addition, unlike bodily injury, invasion of privacy may result in harm which the law finds difficult to characterise and remedy. While in many cases an invasion of privacy will result in serious harm (discussed below) some cases involving ,for example, disclosure of private facts, may involve no more than damaged trust between persons, or between persons and a government agency or firm.[44] Esther Dyson refers to these as 'subjective privacy harms' in which 'the mere knowledge by a second or third party of one's private information is experienced as an injury' in contrast to more tangible harms she calls 'objective harms', such as 'fraud, denial of a service, denial of freedom'.[45]

4.15 In some instances it may not be clear whether the harm to a person's privacy interest arises at the actual point of interference with privacy, or at some later stage when personal information is disclosed to others.[46] In some jurisdictions, the law recognises that mere interference with privacy is a compensable harm.[47] The Australian Law Reform Commission (ALRC) has suggested that this approach is in keeping with the status of privacy as a human right.[48]

4.16 Victoria's *Surveillance Devices Act (1999)* (SDA [Vic]) impliedly recognises that harm results from mere interference with privacy by making it an offence to engage in some non-consensual surveillance of private conversations and activities.[49] The courts have also recognised that interference with privacy interests is a compensable harm. The Victorian Court of Appeal recently awarded damages for breach of confidence to a woman who had suffered mental distress short of psychiatric injury when her former partner circulated a video of them having sex.[50]

4.17 Invasion of privacy is not the only harm that may result from the abuse or overuse of public place surveillance. Writers in the cross-disciplinary field of research known as 'surveillance studies'[51] have identified non-privacy related effects of surveillance. For example, David Lyon, a key surveillance theorist, has complained that 'too often the stock response to issues of surveillance is couched in the language of "privacy"'.[52] According to Lyon, many of the specific anxieties about surveillance are best categorised under other terms, such as 'liberty' (when discussing anxiety about the totalitarian tendencies of government) and autonomy within the marketplace (when discussing commercial surveillance).[53]

4.18 Despite obvious parallels with George Orwell's science fiction novel *Nineteen Eighty-Four* [54] in which the government used public and private surveillance to control the lives of citizens, some observers believe the harms caused by public place surveillance are more likely to be perpetrated by the private sector. Slobogin writes that unlike the novel *Nineteen Eighty-Four,* where individuals could be persecuted by their government for 'thought crimes', persecution from public place surveillance is 'more likely to result in exclusion from certain areas [such as the central business district and shopping centres] than any significant formal punishment'.[55] In other words, surveillance is more likely to serve the interests of business than a totalitarian government in the modern world.[56]

4.19 Because of the widely held belief that surveillance measures may protect against a terrorist threat, Benjamin Goold writes that it is not enough:

> *to allude to the prospect of some dark, totalitarian future as a reason for restricting the use of CCTV. Instead, we must be able to identify definable rights or interests that are threatened by the spread of surveillance cameras.*[57]

4.20 The following risks may be associated with the abuse or overuse of public place surveillance:

- loss of privacy in public places
- loss of anonymity in public places
- possibility of error and a miscarriage of justice
- discriminatory profiling of groups
- voyeuristic uses
- other antisocial uses
- exclusion of groups from public places
- limits to political speech and association
- changes to the nature of public life.

LOSS OF PRIVACY IN PUBLIC PLACES

4.21 Most, if not all, people have reasonable expectations of some privacy in public places. As we discussed in Chapter 3, the nature of those reasonable expectations will change according to the place. For example, most people would reasonably expect that a conversation on a secluded park bench or a quiet beach would not be overheard or recorded, and most people would similarly expect that a brief intimate moment, such as a kiss or embrace, in a secluded public place would not be observed or recorded. It may be unreasonable to have similar expectations on a crowded tram or in the Bourke Street mall.

4.22 Peoples' reasonable expectations of privacy may be breached, or may be capable of being breached, by current public place surveillance practices in Victoria. For example, it was suggested to the commission that audio surveillance is used by half of all buses in the transport sector.[58] A number of businesses also reported that they use cameras to capture images beyond their premises. For example, some retail premises have perimeter cameras that view surrounding parks and public transport areas in order to capture unruly behaviour and motor vehicle theft.[59]

4.23 Some surveillance in public places may intrude upon sensitive matters and activities. For example, in consultations media groups acknowledged that the use of surveillance in public places to collect news worthy stories of public interest that may raise privacy concerns, including stories related to children,[60] family members of public figures,[61] controversial or embarrassing subjects such as drug use and obesity, and images of people grieving.[62]

4.24 The commission also learned about covert forms of surveillance in Victoria,[63] a factor that complicates expectations of privacy. For example, police do not need a warrant to record people's activities in outdoor areas and in busy indoor spaces where people ought reasonably to expect that their activities will be observed.[64]

32 Roundtable 28.

33 Roundtable 16.

34 Roundtable 16 and 18.

35 Roundtables 16 and 28.

36 Roundtable 18.

37 Roundtable 17.

38 Roger Clarke, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

39 *RFID: Frequency, Standards, Adoption and Innovation*, JISC Technology and Standards Watch (May 2006) 22 <www.jisc.ac.uk/media/documents/techwatch/tsw0602.doc> at 18 December 2008.

40 Lisa Martin, 'Stripping for Air Safety', *The Age* (Melbourne), 27 October 2008, Education Section, 12.

41 Asher Moses, 'Google Takes a Risky Road with Privacy', *Sydney Morning Herald* (Sydney), 6 August 2008 <www.smh.com.au/news/web/google-takes-a-risky-road-with-privacy/2008/08/06/1217702095425.html> at 21 January 2009

42 Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 768.

43 Ibid 769.

44 Ibid 770.

45 Esther Dyson, 'How Loss of Privacy May Mean Loss of Security' (2008) 299(2) Scientific American 26, 27.

46 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1* Study Paper 19 (2008) [3.30].

47 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [74.165] referring to Canadian jurisdictions: *Privacy Act 1996* RSBC c 373 (British Columbia) s 1(1); *Privacy Act* CCSM s P–125 (Manitoba) s 2; *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 2; *Privacy Act 1990* RSNL c P–22 (Newfoundland and Labrador) s 3(1).

48 Ibid [74.168].

49 *Surveillance Devices Act 1999* (Vic) ss6 and 7.

50 *Giller v Procopets* [2008] VSCA 236.

51 David Lyon, 'Globalizing Surveillance: Comparative and Sociological Perspectives' (2004) 19 (2) *International Sociology* 135, 146.

52 David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (1994)13.

53 Ibid 13-14.

54 George Orwell, *Nineteen Eighty-Four* (first published 1949, 2000 ed).

55 Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 *Mississippi Law Journal* 213, 251.

56 Ibid 250-251.

57 Benjamin Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance"' (2006) 25 (1) *Criminal Justice Ethics* 3, 5.

58 Roundtable 19.

59 Roundtable 15.

60 Roundtable 27.

61 Roundtable 26.

62 Roundtable 26.

63 Roundtables 5, 25, 26 and 27.

64 This is discussed in detail in Chapter 3..

Chapter 4 Risks and Benefits

4.25 Even when surveillance users do not intend to conceal their activities, failing to ensure that the surveillance is obvious or visible (by using signs for example) effectively makes it covert. The commission was told of numerous instances of surveillance occurring without clear notice to the public.[65] It was noted that, even where signs are used, they do not necessarily contain sufficient information. For example, they may not identify why cameras are used; who owns, operates, or is responsible for them; how footage is managed, where it goes, and the people to whom it can be released; and how to complain about abuse.[66]

4.26 The need to retain privacy in public places is partly concerned with the desire to keep some information private. It could be information we wish to keep secret from people at work, or information we wish to keep secret from those at home. It may relate to our political views, medical matters such as abortion or drug and alcohol treatment, and who we socialise with, such as attendance at a gay bar.[67]

4.27 As noted by Slobogin, 'none of these activities are illegal, but it is easy to imagine why those who engage in them might want to keep them secret'.[68] Jeffrey Reimen warns that losing privacy over such information may mean 'denial of certain benefits, jobs or promotions or membership in formal or informal groups, or even blackmail'.[69]

4.28 Two trends may magnify the risk of harm associated with public place surveillance. One is the internet, which makes the private information uncovered through surveillance widely accessible. For example, a day after the launch of Google Street View in Australia photographs had revealed and exposed to public view 'a lying neighbour, sprung a cheating spouse and snapped a man sleeping on the job'.[70] Solove has noted that young people are particularly vulnerable to these internet-based harms, given the rate at which they post photographs, video and other information about themselves and their friends.[71] He suggests that the consequence of diminished reputation for these young people can be significant:

> *Broad-based exposure of personal information diminishes the ability to protect reputation by shaping the image that is presented to others…We look to people's reputations to decide whether to make friends, go on a date, hire a new employee or undertake a prospective business deal.*[72]

4.29 The second trend which may be increasing the risk of harm from public place surveillance is developments in media culture encouraging privacy invasions. Jennifer Mullaly suggests the following factors are encouraging media invasions of privacy:

- the blurring of the distinction between news and entertainment
- technology's ability to increase the potential for journalistic intrusions into privacy
- competition pushing the boundaries of what is acceptable
- a lack of training for members of the media on victim sensitivity.[73]

LOSS OF ANONYMITY IN PUBLIC PLACES

4.30 The increased use of surveillance may lead to a loss of anonymity in public places. Most, if not all, of us probably take delight in the fact that from time to time we can blend with the crowd and undertake lawful activities with anonymity. In addition, some people may have special grounds for wanting to remain anonymous in public places, for example a person entering a drug rehabilitation clinic.

4.31 Our ability to maintain anonymity with ease in public places is being eroded by the many forms of surveillance, such as tracking devices in mobile phones, use of automated number plate recognition (ANPR) technology to identify cars on toll roads, CCTV surveillance, and individual use of handheld cameras and mobile phone cameras. These practices cause our identities and our locations to become ascertainable as we go about our daily lives in public places.

4.32 One reaction to the loss of anonymity in public places caused by surveillance is to restrict movement in order to avoid unwanted observation. Freedom of movement, like privacy, is a human right protected under international human rights instruments and the Victorian

Charter of Human Rights and Responsibilities Act 2006 (Vic) (the Charter).[74] The Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy, has said that people have the right to exercise their freedom of movement 'without undergoing excessive psychological conditioning' about their movement and conduct, and 'without being the subject of detailed monitoring' through tracking.[75]

POSSIBILITY OF ERROR AND MISCARRIAGE OF JUSTICE

4.33 An important risk associated with increased use of public place surveillance is the possibility of identification error, which may lead to an injustice or damage to reputation. It is often notoriously difficult to accurately identify a person whose image is captured on CCTV footage.[76] This issue arises in facial recognition technology. A 2001 study found that when digitised posed photographs of the same person were taken 18 months apart, the systems would register a 'false rejection' (incorrectly identifying the two photographs as being different people) 43 per cent of the time.[77] While the technology may be improving, observers suggest its capacity for accurately finding faces in a crowd, other than in controlled conditions, is limited.[78]

4.34 Faith in scientific infallibility can stand in the way of a realistic assessment of the effectiveness of surveillance technologies,[79] including when there are human or associated errors. In 2002, the Office of Privacy Commissioner of Canada determined that a bank had released to the police the wrong CCTV footage of a woman the bank believed had cashed stolen cheques.[80] In fact, the bank's computerised central record of transactions at teller stations had been 12 minutes slow, so when it was compared to the CCTV camera (which had the correct time) it suggested that the woman, and not the alleged criminal, had tried to cash the cheques. Friends, family and acquaintances of the women would later see her photograph in a local daily newspaper as part of an article on 'Crime of the Week'.

4.35 More recently, the UK newspaper the *Guardian* reported that a young mother in the town of Middlesbrough, UK, appeared on television news after CCTV operators incorrectly believed that she had thrown litter to the ground. In fact, she had just bought chips for her daughter and had crumpled the packet and placed it in the bottom of her daughter's pram.[81]

65 Including for example Roundtables 3, 4, 10, 11, 14, 15. 24, 25.

66 Roundtable 16.

67 Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 *Mississippi Law Journal* 213, 244-245.

68 Ibid 245.

69 Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Computer and High Technology Law Journal* 27, 35.

70 Asher Moses, 'Google Takes a Risky Road with Privacy', *Sydney Morning Herald* (Sydney), 6 August 2008 <www.smh.com.au/news/web/google-takes-a-risky-road-with-privacy/2008/08/06/1217702095425.html> at 21 January 2009.

71 Daniel Solove, 'The End of Privacy?' (2008) 299 *Scientific American* 79, 81.

72 Ibid 81.

73 Jennifer Mullaly, 'Privacy: Are the Media a Special Case?' (1997) 16 (1) *Communication Law Bulletin* 10, 10-11.

74 See *International Covenant on Civil and Political Rights*. opened for signature 16 December 1966, 999 UNTS 171, art 17 (entered into force 23 March 1976); and *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 12.

75 Article 29 Data Protection Working Party, European Commission, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance* Adopted on 11 February 2004:11750/02/EN: WP89 (2004) 6.

76 For example, in our consultations with businesses, we were told that police will not act in relation to an incident caught on CCTV unless the images are clear: Roundtable 20.

77 Tom Gorman, Charles Piller, and Josh Meyer, 'Criminal Faces in the Crowd Still Elude Hidden ID Cameras', *Los Angeles Times* (Los Angeles), 2 February 2001 <http://articles.latimes.com/2001/feb/02/news/mn-20035> at 21 January 2009.

78 See Ashley Phillips, Researchers Develop 100% Accurate Electronic Face Recognition: *Critics Call Technology Unreliable and Invasion of Privacy* (24 January 2008) ABC News <http://abcnews.go.com/Technology/Story?id=4183902&page=1> at 21 January 2009; and Mike Thompson, Linus Information Security Solutions (Speech delivered at the [Id]entity 08 Conference, Melbourne, 12 November 2008).

79 Interview with Mike Thompson (Telephone interview, 3 December 2008).

80 *Commissioner's Findings, PIPEDA Case Summary #53, Bank Accused of Providing Police With Surveillance Photos of the Wrong Person*, Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/2002/cf-dc_020628_1_e.asp> at 16 December 2008.

81 Martin Wainwright, 'Talking CCTV Cameras Accuse the Wrong Person', the *Guardian* (London), 12 April 2007 <www.guardian.co.uk/uk/2007/apr/12/ukcrime.humanrights> at 26 June 2008.

4.36 Examples from Australia include:

- a parking permit agency reportedly denying a permit to someone in New South Wales because satellite images showed a parking space in the back of their house. In fact, the agency had been looking at the wrong house.[82]
- concern expressed by the Victorian Privacy Commissioner that the hotlist of wanted cars against which CrimTrac's proposed national ANPR system would compare number plates may not be kept up to date and could thus lead to errors.[83]
- concerns expressed in consultations that CCTV footage generally only shows who entered a particular area, and not the actual incident of interest.[84]

DISCRIMINATORY PROFILING OF GROUPS

4.37 Public place surveillance is vulnerable to discriminatory use through targeting of individuals because of their membership of a particular cultural or ethnic group. This activity is known as 'profiling', a technique in law enforcement where police rely on personal traits (such as race, gender and age) to target potential offenders. Profiling is unfair, it may violate anti-discrimination laws and it may be a threat to social cohesion.[85]

4.38 Clive Norris and Gary Armstrong conducted an important study demonstrating discriminatory profiling using public place surveillance between 1995 and 1996. The researchers sent observers to monitor CCTV operators in three shopping areas in Britain in order to determine how the operators selected individuals for CCTV camera scrutiny.[86] The results showed that operators often lacked a reasonable basis when they used CCTV, relying instead on attributes such as race, class, gender and age.

4.39 For example, the study found that black people were between one-and-a-half to two-and-a-half times more likely to be targeted for surveillance than their numbers in the population would have suggested.[87] In addition, the disproportionate targeting was not necessarily explained by higher offending rates. While black people made up 32 per cent of those targeted by surveillance, they were only nine per cent of those arrested.[88] More generally, the authors cite studies suggesting that offending is far more evenly distributed in the population than in official statistics, and that race and class differentials disappear when you ask young people directly about their past offending behaviour.[89]

4.40 The authors also found more direct evidence of racism among the operators:

> *Although only used by a minority, the terms "Pakis," "Jungle Bunnies" and "Sooties" when used by some operatives did not produce howls of protests from their colleagues or line managers. Stereotypical negative attitudes towards ethnic minorities and black youths in particular were more widespread. These attitudes ranged from more extreme beliefs, held by a few operators, about these groups' inherent criminality to more general agreement as to their being "work-shy," or "too lazy" to get a job, and in general, "trouble".*[90]

According to the authors, 'some of the white operators targeted blacks with a relish that implied a deep prejudice'.[91] Moreover, at one site, targeting of blacks was a 'deliberate matter of policy' with operators told that the priority target was black youths.[92]

4.41 In addition to racial profiling, operators also engaged in discriminatory profiling based on gender, age and class. The authors found that teenagers and men were about twice as likely to be targeted by operators for CCTV scrutiny than what their numbers in the population would have suggested.[93] The authors discovered that operators had a negative view towards youth generally, but particularly 'those identified – by attire, location, or body language – as poor or belonging to the under-class'.[94]

4.42 The report's authors found that women 'were almost invisible to the cameras'.[95] Women were not targeted for criminal propensity, or for protective purposes.[96] Moreover, the authors found that CCTV reproduced many of the gender stereotypes found in society, including the failure to acknowledge domestic violence. As an example, the authors describe an instance in which a man striking his female companion on the street did not

illicit a law enforcement response from operators. According to the authors: 'lesser assaults, when perpetrated by men on men outside nightclubs, resulted in police officers being deployed and arrests being made.'[97]

4.43 The authors found that the most common reason for operators selecting an individual for greater scrutiny was for 'no obvious reason', rather than any specific behaviour.[98]

4.44 It is unclear whether discriminatory behaviour exists among CCTV control operators in Australia, although it has been suggested that it may.[100] One study of the Gold Coast Safety Camera Network found those targeted were overwhelmingly male (94 per cent) and young (74 per cent).[101]

4.45 In our consultations it was suggested that public place surveillance may disproportionately affect or target some members of the community. For example, in a number of our roundtables, it was noted that young people are more impacted by public place surveillance, because of their greater use of public places.[102] In other roundtables, more deliberate targeting of youth was noted, as well as culturally and linguistically diverse communities, homeless people and people with a mental illness.[103] In the Indigenous justice roundtable, a participant noted that the community feels monitored by police when they attend Koori events.[104]

VOYEURISTIC USES

4.46 Public place surveillance may be used for voyeuristic and even sexually abusive purposes.[105] For example, a group of male teenagers recorded a sexual attack in Werribee on a developmentally delayed 17-year-old girl and sold the DVD in schools.[106] Mobile phones have been used by children as a means of bullying in Australia as well as overseas.[107] For example, in Japan, an overweight boy was covertly photographed in the school change room and his picture sent to his classmates' phones for ridicule.[108]

4.47 Some people have used covert cameras [109] to photograph beneath women's skirts, a practice known as 'upskirting'.[110] Cameras have been secretly installed in toilets and change rooms to view persons showering or dressing.[111] Cameras have also been used covertly to create child pornography. For example, a man was prosecuted for making pornographic videos of young girls changing at the Harold Holt swimming pool in Melbourne's east.[112]

82 Pauline Wright, 'How Well do the ALRC/NSWLRC Proposals Contribute to Limiting the Growth of a Surveillance Society?' (Paper presented to the Cyberspace Law and Policy Centre Symposium: Meeting Privacy Challenges: The ALRC and NSWLRC Privacy Reviews, Sydney, 2 October 2008; and '"Big Brother" Council Watching Sydneysiders?', ABC News, 18 September 2008 <www.abconline.net.au/news/stories/2008/09/18/2367812.htm> at 15 January 2009.

83 Helen Versey, 'Location Privacy: The Privacy Regulator's Perspective' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

84 Roundtable 16.

85 On the threat to social cohesion see Clive Norris and Gary Armstrong, 'CCTV and The Social Structuring of Surveillance' in Kate Painter and Nick Tilley (eds) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention* (1999) 176.

86 Ibid 160.

87 Ibid 162.

88 Ibid 172.

89 Ibid 175.

90 Ibid 169.

91 Ibid 171.

92 Ibid 171.

93 Ibid 162.

94 Ibid 164.

95 Ibid 172.

96 Ibid 172.

97 Ibid 173.

98 Ibid 163.

99 Ibid 159.

100 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 3; Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* (2003) 102 citing Phil Crane and Mike Dee, 'Young People, Public Space and New Urbanism' (2001) 20(1) *Youth Studies Australia* Vol 11, 11–18.

101 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 40. Figures have been rounded to the nearest whole number.

102 Roundtables 2 and 7.

103 Roundtables 16, 17, and 18,

104 Roundtable 28.

105 See Tony Eastley, 'Video of alleged rape raises concerns about use of mobile phones', *AM*, 5 April 2007, <www.abc.net.au/am/content/2007/s1890486.htm> at 21 May 2008; Daniella Miletic and David Rood, 'Boys sell film of girl's humiliation', *Sydney Morning Herald* (Sydney) 25 October 2006, 3.

106 'Hi-tech Cops Use Cyber Clues', *The Advocate* (Melbourne), 1 April 2008, 16 <theadvocate.yourguide.com.au/news/local/news/general/hitech-cops-use-cyber-clues/371166.aspx#> at 16 January 2009.

107 See Marilyn Campbell, 'Cyber Bullying: An Old Problem in a New Guise?' (2005) 15(1) *Australian Journal of Guidance and Counselling* 68-76 <eprints.qut.edu.au/archive/00001925/01/1925.pdf> at 21 May 2008.

108 Alanna Mitchell, 'Bullied by the Click of a Mouse', *Globe and Mail* (Canada), 24 January 2004 <www.theglobeandmail.com/servlet/story/RTGAM.20040124.wbully0124/BNStory/Front/> 22 January 2009

109 See Georgie Pilcher, 'Sneaker Peeker Bootcam Videos up Skirts', *Herald Sun* (Melbourne), 18 January 2007, 13.

110 Steve Butcher, 'Student jailed for 'upskirting' at tennis', *The Age* (Melbourne), 6 June 2007, 12.

111 See Kate Uebergang, 'Prison term cut for toilet spy', *Herald Sun* (Melbourne), 14 November 2007, 2; Mark Russell, 'The Spying Game: Privacy Threatened by Rise in Hidden Cameras', *The Sunday Age* (Melbourne), 30 September 2007, 7.

112 Katie Lapthorne, 'Order on video voyeur', *Herald Sun* (Melbourne), 14 June 2003, 7.

Chapter 4 Risks and Benefits

4.48 Websites now exist where people are posting embarrassing shots gathered from Google Street View, including some that show women sunbathing.[113] Privacy advocates have expressed concerns that images from taxi surveillance cameras that have captured people in the back of the taxi engaged in sexual conduct could end up on the internet.[114]

4.49 There is also evidence of voyeuristic use of CCTV systems in public places. In their study of CCTV operators at three shopping centres in the United Kingdom, Norris and Armstrong have said that 'with its pan-tilt and zoom facilities, the thighs and cleavages of scantily clad women are an easy target for those male operators so motivated'.[115] They found that 10 per cent of all targeted surveillances on women in their study were for voyeuristic reasons.[116] An example of CCTV used for voyeuristic purposes identified in the study was the use of a camera to capture footage of prostitutes and their clients meeting in an alley. According to one camera operator cited in the study:

> *police officers in the communications office enjoy such scenarios and, when bored, will sometimes phone to ask him to put the cameras on Shaggers Alley for their titillation and they were also told of a "Shaggers Alley greatest hit tape".*[117]

4.50 We have previously referred to the trial use in some Australian airports, including Melbourne, of x-ray security scanners that allow screeners to see through a person's clothing and view their external organs and genitals.[118] According to Stephen Blanks of the New South Wales Council for Civil Liberties, the device conducts a virtual strip search and provides detailed images of a person's body shape that many people might find highly embarrassing.[119] *The Age* reported:

> *Women in particular have expressed concerns about the trial. "I am overly concerned with women's privacy and the introduction of these machines. I'm very sorry but I would feel horrendously embarrassed to have any sanitary products revealed on the scanner" a* Herald Sun *reader wrote. Others are concerned about security staff looking at images of child passengers being screened.*[120]

OTHER ANTISOCIAL USES OF SURVEILLANCE EQUIPMENT

4.51 There are reports of other antisocial or undesirable uses of surveillance equipment in public places. For example, the American Civil Liberties Union (ACLU) has described instances of police abuse such as when a top-ranking police official in Washington DC looked up the license plate numbers of cars parked at a gay club and matched them to the vehicle owners to try to blackmail patrons who were married.[121] The ACLU also cites an investigation by the Detroit Free Press which showed Michigan police using a database 'to help their friends or themselves stalk women, threaten motorists after traffic altercations, and track estranged spouses'.[122]

4.52 There is also a practice known as 'happy slapping' in which people use mobile phones to film random attacks or assaults on strangers, usually for the purpose of distribution to friends or publication on the internet.[123] One example of happy slapping is the case involving a 14-year-old girl who filmed a bar manager as he was being beaten in the UK. The man died from his injuries. Footage of the attack was sent to friends' mobile phones and published on the internet. The girl was jailed for her role in filming and participating in the attack.[124]

4.53 The potential for harm from the antisocial use of surveillance equipment is magnified by the phenomenon of 'purpose creep'. Purpose creep, also known as 'function creep', occurs when a surveillance practice undertaken for one purpose is used for other purposes.[125] An example of purpose creep mentioned during our consultations is the use of systems designed to address serious crimes to focus on individuals 'being a nuisance or merely looking suspicious'.[126]

EXCLUDING GROUPS FROM PUBLIC PLACES

4.54 Commentators have expressed concern that the abuse or overuse of public place surveillance may cause specific groups in society, such as young people, the poor and the homeless, to be excluded from some public places. Exclusion may result from CCTV camera operators targeting members of these groups or behaviour, short of criminality, that some group members may be more likely to engage in.

4.55 For example, Jeffrey Rosen has suggested that in Britain CCTV is used less to thwart serious crime and more to enforce social conformity, such as keeping punks out of shopping malls.[127] In Melbourne, CCTV deployment in the central business district has been closely associated with concerns about drunkenness.[128] In consultations, local councils in Victoria told the commission they use CCTV to target street-car racing, drunk and disorderly behaviour, sale of tobacco to underage children,[129] skateboarding and graffiti.[130]

4.56 Evidence that these uses of CCTV lead to the exclusion of certain groups from public places is varied. Norris and Armstrong, in their study of CCTV operators, found that the operators were discriminatory as to whom they targeted with their cameras, however they acknowledged that the behaviour did not necessarily lead to further action such as requesting police or security guard attendance at the scene, or arrest.[131] On the other hand, Mike McCahill found evidence of exclusion in his study of CCTV operators at two shopping complexes. Specifically, he found that four out of ten teenagers to whom a guard was directed to approach were ejected from the shopping centres under study.[132] He also noted many of these exclusions may be described as 'profile-based' exclusions.[133]

4.57 One theory about the use of CCTV to address 'undesirable' behaviour ties it to the aim to create public spaces conducive to commercial activity. According to Heidi Mork Lomell, 'to create attractive and seductive consumer spaces, cities must not only reduce crime, but also forms of conduct that might "put customers off" and, in practice, this means excluding "undesirables"'.[134] Indeed, Lomell further notes that studies suggest that operators look not just for potential criminals, but also for potential non-consumers.[135] For example, McCahill's study concluded that 'the main preoccupation of the

113 Chris Rizos, 'Location Based Services and Issues such as Privacy' (Speech delivered at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

114 Mark Russell, 'Back-Seat Fun: Careful They Might Film You' *The Age* (Melbourne), 8 July 2007, 2, <www.theage.com.au/news/national/careful-they-might-film-you/2007/07/07/1183351523691.html> at 22 January 2009.

115 Clive Norris and Gary Armstrong, 'CCTV and The Social Structuring of Surveillance' in Kate Painter and Nick Tilley (eds) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention* (1999) 174.

116 Ibid 174.

117 Ibid 174-175.

118 'Australian Airport Trials Full-Body X-Rays', *The Australian* (Sydney), 2 October 2008 <www.theaustralian.news.com.au/story/0,25197,24432963-5006787,00.html> at 16 January 2009.

119 Ibid.

120 Lisa Martin, 'Stripping for Air Safety', *The Age* (Melbourne), 27 October 2008, Education Section 12 <www.education.theage.com.au/pagedetail.asp?intpageid=2089&strsection=&intsectionid=0> at 19 January 2009.

121 *What's Wrong With Public Video Surveillance?*, American Civil Liberties Union <www.aclu.org/privacy/spying/14863res20020225.html> at 19 January 2009.

122 Ibid.

123 See, eg, Liam Houlihan, 'Teen assaults filmed for web', *Herald Sun* (Melbourne), 30 April 2005, 9.

124 See 'Girl, 14, killer in 'happy slapping'', *The Australian* (Sydney), 25 January 2006, 10; 'Stark Warning over Happy Slapping', BBC News (UK), 18 March 2008, <http://news.bbc.co.uk/2/hi/uk_news/england/7293829.stm> at 28 January 2009 ; 'Happy Slap Accomplice Sentenced', BBC News (UK), 18 March 2008, <http://news.bbc.co.uk/2/hi/uk_news/england/bradford/7302959.stm> at 28 January 2009.

125 'Eyes on the Road', *The Age –Good Weekend* (Melbourne), 3 February 2006 <www.theage.com.au/news/technology/how-they-keep-track-of-our-every-move/2006/02/03/1138836402623.html?page=fullpage#contentSwap2> at 20 January 2009 quoting Roger Clarke.

126 Roundtable 18.

127 Jeffrey Rosen, 'A Watchful State', *New York Times Magazine* (New York), 7 October 2001 <query.nytimes.com/gst/fullpage.html?res=9505E4DE123DF934A35753C1A9679C8B63&sec=&spon=&pagewanted=all> at 15 January 2008.

128 Kate Lahey, 'Spy in the Street: Nixon's Answer to Violence After Dark', *The Age* (Melbourne), 11 November 2008, 1–4.

129 Roundtables 6, 7 and 8.

130 Roundtable 6.

131 Clive Norris and Gary Armstrong, 'CCTV and The Social Structuring of Surveillance' in Kate Painter and Nick Tilley (eds) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention* (1999) 175-176.

132 Mike McCahill, *The Surveillance Web: The Rise of Visual Surveillance in an English City* (2002) 146.

133 Ibid147.

134 Heidi Mork Lomell, 'Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway' (2004) 2 (2/3) *Surveillance & Society* 346, 346.

135 Ibid 347.

security personnel was the monitoring and exclusion of groups of youth who disrupted the commercial image'.[136] Lomell concludes that CCTV, along with the 'commercialization of public space':

> *have the effect of excluding people incapable of consuming, people who might fail to participate in or might actively disturb the main activity of the area, namely shopping.*[137]

4.58 Participants in our consultations suggested that CCTV can exclude certain groups from public places. For example, there have been complaints by youth about being 'moved on' when congregating in public areas.[138] It was also suggested that in an effort to combat drug traffic, police are seeking court orders that would exclude a person from an area or city.[139] Some community organisations noted that their clients report difficulties at shopping centres where CCTV is used to look for everything from theft to inappropriate language, to being a nuisance and merely looking suspicious.[140]

4.59 The possible exclusion of some people from public places raises a number of concerns. Jason Patton has noted that public places promote social cohesion and act as a sort of social glue ensuring that people of various backgrounds have shared experiences.[141] He notes the views of Frederick Law Olmsted who in designing New York's Central Park, believed the natural landscape would inspire communal feelings among an otherwise socially stratified and class-based society.[142]

4.60 Patton suggests that public places promote a sense of belonging to society. According to Paton 'everyone who counts as a member of the public has the right to present themselves in public space',[143] and:

> *negotiations over the behaviours allowed in public places are highly political because they legislate who counts as the public and who is allowed to be a part of the community.*[144]

4.61 A strategy that excludes people who engage in undesirable behaviour in public places also fails to address the underlying causes of the behaviour. It may also 'crowd out' measures that address underlying causes, such as creating recreational spaces for young people and providing mental health care for homeless people with mental illness or addressing drug abuse. It may also threaten community policing strategies. Nik Theodore has written that surveillance as a form of 'remote policing' can alienate or disconnect police officers 'from the marginalized communities they are charged to protect'.[145]

4.62 Finally, the risk that certain people will be denied access to public space is magnified by the increase in privately owned public places, such as shopping centres and entertainment complexes. Walter Siebel and Jan Wehrheim suggest that the temptation to move along 'undesirables' may be acted upon with less public accountability in the case of private public places than would be the case with police on city streets.[146]

CHILLING POLITICAL SPEECH AND ASSOCIATION

4.63 Awareness of the widespread existence of surveillance equipment may have the capacity to 'chill' dissent. This occurs where speech or conduct by individuals is suppressed by the knowledge that it may result in undesirable consequences.

4.64 The use of surveillance to stifle dissent has typically been associated with totalitarian regimes, such as in Eastern Europe prior to the collapse of the Soviet Union. George Orwell's classic text *Nineteen Eighty-Four*[147] provides a fictional illustration of 'thought police' monitoring individuals through 'telescreens'.[148]

4.65 In Victoria, political activists have been subject to various forms of police surveillance, including camera surveillance at demonstrations, and, in at least one instance, publication of photographs of protestors in a newspaper.[149] We also learned in consultations that police have recommended that certain local councils use cameras to monitor political demonstrations.[150] *The Age* reported that Victorian police have placed undercover agents within a number of activist organisations.[151] In consultations, the commission was told that some members of the community have concerns about being subject to surveillance when at protests, demonstrations and other large gatherings.[152]

4.66 The European Parliament's Civil Liberties Committee has written that 'surveillance technologies exert a powerful chilling effect on individuals who wish to dissent, and [may] deter these individuals from exercising their democratic right to protest government policy'.[153]

CHANGING THE NATURE OF PUBLIC LIFE

4.67 Finally, some commentators have suggested that the loss of privacy and anonymity in public places will lead to subtle changes in public behaviour, resulting in a less individual, relaxed and interesting society.[154]

4.68 The notion that surveillance may lead to subtle changes in human behaviour is well illustrated by social reformer Jeremy Bentham's design for a prison called the 'Panopticon'. The Panopticon was a model for a prison in which individual prison cells surrounded a central inspection tower.[155] The use of blinds in the central inspection tower meant that the inspector could see out, but the prisoners could not see the inspector.[156] This structure was vital, as Bentham believed that the prisoners' uncertainty about whether or not they were being watched caused them to adapt their behaviour in a self-disciplinary way.[157] According to a popular account of the Panopticon:

> *the true genius of the idea lay in what made it, in [Bentham's] words, "a new mode of obtaining power of mind over mind." Because the prisoners would not be able to see whether a guard was in the Panopticon's tower, it could often be unmanned and they would never know. Out of fear and uncertainty, the prisoners would in effect stand watch over themselves.*[158]

4.69 Bentham was ultimately unable to persuade the British government to approve the final construction of the prison,[159] but years later the French philosopher Michel Foucault borrowed the concept of the Panopticon to describe how modern social institutions—including factories, hospitals, the military and schools—use surveillance to control the populace without the use of force.[160] According to Lyon, Foucault argued that:

> *modern societies have developed rational means of ordering society that effectively dispense with traditional methods like brutal punishment. Rather than relying on external control and constraints, modern social institutions employ a range of disciplinary practices which ensure that life continues in a regularized, patterned way.*[161]

4.70 Alan Westin writes that 'knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.'[162] According to Slobogin, the small amount of social science research about this phenomenon confirms that when people believe they are stared at, they feel disquiet. For example, he notes a research finding that 'monitored employees are likely to feel less trusted, less motivated, less loyal and more stressed than employees who are not subject to surveillance' although he acknowledges that it remains unclear if these effects would also be present in public places.[163]

136 Mike McCahill, *The Surveillance Web: The Rise of Visual Surveillance in an English City* (2002) 147.

137 Heidi Mork Lomell, 'Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway' (2004) 2 (2/3) *Surveillance & Society* 346, 347.

138 Roundtable 16.

139 Roundtable 16.

140 Roundtable 18.

141 Jason Patton, 'Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places' (2000) 2 *Ethics and Information Technology* 181, 183.

142 Ibid, 183 discussing Geoffrey Blodgett, 'Frederick Law Olmsted: Landscape Architecture as Conservative Reform' (1976) 62(4) *Journal of American History* 869, 878.

143 Ibid 183.

144 Ibid 183.

145 Nik Theodore, et al, 'Securing the City: Emerging Markets in the Private Provision of Security Services in Chicago' (2006) 33 (3) *Social Justice* 85, 96.

146 Walter Siebel and Jan Wehrheim, 'Security and the Urban Public Sphere' (2006) 3 (1) German Policy Studies 19, 22.

147 George Orwell, *Nineteen Eighty-Four* (first published 1949, 2000 ed).

148 Ibid 5.

149 Dan Oakes, 'Furore Over G20 "People of Interest" Photos', *The Age* (Melbourne), 19 January 2007, 6.

150 Roundtable 7.

151 Richard Baker and Nick McKenzie, 'How Police Spy on Foes of War, Whaling and Battery Hens', *The Age* (Melbourne) 16 October 2008, 1.

152 Roundtable 16.

153 Arthur Cockfield, 'Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance' (2003) 29 *Queens's Law Journal* 364, 396. Note that the report focuses states use of surveillance technologies pursuant to national interest-type rationales.

154 See eg, Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Computer and High Technology Law Journal* 27; Edward Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962.

155 David Lyon, *Surveillance Studies: An Overview* (2007) 57.

156 Ibid 57.

157 Ibid 59.

158 John Rennie, 'Here in the Fishbowl' (2008) 299(3) *Scientific American* 8, 8.

159 Bentham did not succeed in getting the British government to approve final construction of the prison. John Rennie, 'Here in the Fishbowl' (2008) 299(3) *Scientific American* 8, 8.

160 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 (4) *British Journal of Sociology* 605, 607.

161 David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (1994) 7.

162 Alan Westin, *Privacy and Freedom* (1967) 31.

163 Christopher Slobogin, 'Public Privacy: Camera

Chapter4 Risks and Benefits

4.71 Another noted effect of public place surveillance is to foster suspicion in society.[164] Marcus Wigan and Roger Clarke write that surveillance 'signals that powerful organisations distrust people, and it encourages distrust by people of one another, and of organisations'.[165] The Surveillance Studies Network additionally writes:

> *The employer who installs keystroke monitors at workstations, or GPS devices in service vehicles is saying that they do not trust their employees … And when parents start to use webcams and GPS systems to check on their teenagers' activities, they are saying they don't trust them either.*[166]

Social relationships, the Network writes, 'depend on trust and permitting ourselves to undermine it in this way seems like a slow social suicide'.[167]

4.72 It has been suggested that the abuse or overuse of surveillance may lead to less diverse and more normalised behaviour in society. According to Sheri Alpert, this is because 'individuals often change their behaviour to conform to what they believe those monitoring their movements/actions will find "acceptable" or "normal"'.[168] Similarly, Reimen writes:

> *When you know you are being observed, you naturally identify with the outside observer's viewpoint, and add that alongside your own viewpoint on your action. This double vision makes your act different, whether the act is making love or taking a drive. The targets of the panopticon know and feel the eye of the guard on them, making their actions different than if they were done in private. Their repertoire of possible actions diminishes as they lose those choices whose intrinsic nature depends on privacy.*[169]

4.73 Jerry Kangwrite has suggested that surveillance may lead to a reduction in original thinking, deliberation and experimentation:

> *excessive inhibition—not only of illegal activity but also of legal, but unpopular, activity—can corrode private experimentation, deliberation, and reflection. The end result may be bland, unoriginal thinking or excessive conformity to unwarranted social norms… [that] sap an individual's ability to question the status quo and to experiment with alternate conceptions of the good life.*[170]

4.74 Edward Bloustein has argued that this results in the loss of individuality:

> *The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual.*[171]

4.75 Reimen writes of the impact of surveillance on our personalities in the following terms: 'the risk…is not that we shall lose something we now enjoy, but that we will become something different than we currently are, something less noble, less interesting, less worthy of respect.'[172] He suggests, for example, that what we become is more infantile as there is a 'widely recognized correlation between privacy and adulthood'.[173]

4.76 Finally, Reiman links the normalisation of personality to our ability to resist oppression:

> *To say that people who suffer this loss* [of personality] *will be easy to oppress doesn't say enough. They won't have to be oppressed, since there won't be anything in them that is tempted to drift from the beaten path or able to see beyond it.*[174]

THE BENEFITS OF PUBLIC PLACE SURVEILLANCE

4.77 Despite the risks, some of which are significant, public place surveillance also appears to offer important benefits. Some of the key benefits are detailed below.

SAFETY

4.78 One of the clear benefits of much public place surveillance is to promote community safety. We noted in Chapter 2 that the transport sector and some businesses use CCTV to manage crowds and respond to accidents. Tracking devices in mobile telephones are used by some parents to keep track a child's whereabouts[175] and by carers for tracking people suffering from memory loss.[176] The GPS systems in mobile telephones can assist in emergencies, such as locating an unconscious person.[177]

CONVENIENCE

4.79 Another important benefit of some forms of surveillance is convenience. In Chapter 2 we referred to the example of the use of RFID in keys to locate and identify cars, and the use of RFID by businesses to identify a product buried within packaging. Some surveillance technologies can also speed up travel, including ANPR on toll roads and facial recognition technology at airports.[178] GPS technology in mobile phones may assist consumers to find nearby services, while the same technology in cars assists with navigation.

4.80 The Surveillance Studies Network has noted the power of surveillance to assist in many aspects of modern life:

> *Surveillance can certainly help to create many new services, and a speeded-up urban lifestyle characterised by individually tailored services, continuous electronic and physical interaction, an always-on digital economy, and the transcendence of many of the time and space barriers that traditionally acted to inhibit urban life.*[179]

CRIME CONTROL

4.81 The most noted benefit of CCTV is its role in protecting against crime, with media stories appearing regularly in Victoria about proposals for more CCTV to deter or solve a variety of crimes. According to Helene Wells and others, CCTV is thought to control crime in at least five ways:

1. preventing crime and disorder by acting as a psychological deterrent
2. aiding in the detection of crime and disorder by police or security personnel
3. increasing the apprehension and successful prosecution of offenders through the effective deployment of police and the gathering of evidence
4. reassuring the public and providing a sense of safety or reduced fear of crime
5. acting as a general site management tool that assists police and security personnel to better manage locations.[180]

4.82 Other ways in which CCTV may reduce crime is by increasing the number of people who frequent a place (because of an increased sense of safety from CCTV), thereby creating 'natural surveillance' that deters offenders; deterring crime by creating publicity that crime is now being taken seriously; and acting as a prompt reminding people to take measures such as locking up their car.[181]

164 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [2.8.2].

165 Marcus Wigan and Roger Clarke, 'Social Impacts of Transport Surveillance' (2006) 24 (4) *Prometheus* 389, 390.

166 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) [2.8.2].

167 Ibid [2.8.2].

168 Sheri Alpert, 'Privacy and Intelligent Highways: Finding the Right of Way' (1995) 11 *Santa Clara Computer and High Technology Law Journal* 97, 106.

169 Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Computer and High Technology Law Journal* 27, 38.

170 Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50 *Stanford Law Review* 1193, 1216–1217.

171 Edward Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962,1003.

172 Jeffrey Reiman, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Computer and High Technology Law Journal* 27, 40.

173 Ibid 40.

174 Ibid 42.

175 See, eg, 'Tracking teens: Parents use GPS Cell Phones to Keep up with Their Children' LA Times/Washington Post wire service, 27 June 2006, <medialab.semissourian.com/story/1158246.html> at 30 June 2008.

176 See Katina Michael, Andrew McNamee, MG Michael, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring' *Faculty of Informatics Papers,* University of Wollongong <ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers> at 21 May 2008.

177 Chris Rizos, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Speech delivered at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008).

178 Australian Customs Service, *Benefits* (2007) <www.customs.gov.au/site/page.cfm?u=5554> at 22 January 2009.

179 David Wood (ed), Surveillance Studies Network, *A Report on the Surveillance Society* (2006) 38..

180 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 1.

181 Nick Tilley, *Crime Prevention Unit Paper No 42 — Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities* (1993) 3-4.

Chapter 4 Risks and Benefits

CCTV's effectiveness

4.83 Evidence that CCTV is effective in controlling crime remains largely inconclusive.[182] Researchers have concluded that CCTV is 'either largely ineffective at reducing crime or that CCTV has different effects depending on the type of crime under consideration'.[183] Brandon Welsh and David Farrington concluded in 2002 that 'the best current evidence suggests that CCTV reduces crime to a small degree'.[184]

4.84 Welsh and Farrington conducted a systematic review of 19 studies from the US and the UK. The authors found a statistically significant but small 'positive' effect from CCTV on crime rates. That is, crime either decreased more in the area with CCTV relative to the area without CCTV, or else it increased more in the area without CCTV relative to the area with CCTV.[185] Among the 19 studies, 10 showed such a positive effect, and nine failed to show a positive effect.[186]

4.85 In 2005 an evaluation of 13 CCTV projects in various locations in the UK (including town centres, city centres, car parks and residential areas) found that only two of the 13 systems showed a statistically significant reduction in crime relative to neighbouring areas without CCTV.[187] Moreover, in one of these two systems the reduction could be explained by a factor other than CCTV.[188] The authors concluded that in their study CCTV had 'mostly failed to reduce crime'.[189]

4.86 In Australia, there have been few published evaluations of CCTV. Dean Wilson and Adam Sutton noted in 2003 that 'where systems have been evaluated this has tended to be in-house' and that of the six evaluations of open-street CCTV systems in Australia as at October 2002, only two were publicly available.[190] In 2006, Wells and others published results from their research into CCTV use in Gold Coast public spaces and on the Queensland Rail Citytrain network.[191] The authors found an increase in total offences against the person after CCTV had been installed as compared to areas without CCTV.[192] They concluded that it was likely that CCTV detected violent crime that previously went undetected, but it had not prevented it.[193]

4.87 Even when CCTV has been shown to reduce crime rates, that reduction relates to certain types of crimes only. For example, CCTV has been more successful at reducing property crimes[194] with two studies finding that CCTV was especially effective at reducing vehicle theft from car parks.[195] CCTV may be less effective at reducing crime against the person and 'impulsive' acts such as alcohol-related crime.[196] Wells and others also report that the evidence of CCTV's effectiveness at reducing burglary is mixed, and CCTV may have no impact on shoplifting.[197] A recent episode of the Australian Broadcasting Corporation (ABC) television program *Catalyst* questioned whether CCTV can prevent terrorist attacks.[198]

4.88 Researchers have also noted the possibility that some decline in crime rates after CCTV is installed may be due to a 'displacement' effect rather than a true decline in the overall crime rate. Displacement occurs when incidents of crime move to areas not covered by CCTV. Research conducted in the Devonport area of Tasmania found that while the incidence of burglary in streets in which CCTV cameras were operating dropped significantly, there was a concurrent increase in burglaries in neighbouring streets without CCTV systems.[199] Similarly, it was suggested in consultations that one response to CCTV use in Melbourne has been that drug deals have moved elsewhere.[200] Nevertheless, Wilson and Sutton argue the statistical evidence on displacement effects from CCTV is largely inconclusive.[201]

4.89 CCTV may also have a limited capacity to assist with criminal apprehension and prosecution. For example, Martin Gill and Angela Spriggs write that 'early concerns that CCTV might become a substitute for police officers do not appear to have been realised'.[202] For example, the public still appear to prefer police on the beat.[203] In addition, while there have been a number of reported examples of its successful use in identifying suspects,[204] an analysis from London, where the UK government has made a substantial investment

in CCTV, found no link between a high number of CCTV cameras in a given location and improved crime clear-up rates.[205] Gill and Spriggs also note difficulties associated with using CCTV evidence in court in part due to 'information overload'.[206] Finally, the European study of CCTV discussed earlier concluded that CCTV has a limited role in crime detection.[207]

4.90 CCTV effectiveness also appears to be highly dependent on the type of system used, its location,[208] and whether used in conjunction with other crime prevention methods[209] such as private security officers and police.[210] Indeed, while recommending that businesses consider using CCTV to prevent burglaries, a Department of Justice publication notes that offenders identify the presence of security guards and whether premises surrounding the targeted premises are occupied as 'the most effective deterrents to prevent burglary'.[211] CCTV effectiveness also ultimately depends on the human operators who monitor them, with a study reportedly finding that operators can concentrate for only about five minutes before their attention starts to wander.[212]

4.91 CCTV systems can also be circumvented. For example, Mike Thompson notes that smart cards and fingerprint technology used at airports can be circumvented by something as simple as stealing the smart card from the user before he or she is to pass through the gate.[213] Similarly, in our consultations, some private security groups told the commission that professional perpetrators of crime worked around CCTV cameras,[214] and young people told us that individuals avoided detection by public transport CCTV systems by positioning themselves under the cameras.[215]

4.92 Some opinion surveys suggest that the public is aware of the possibly limited effectiveness of CCTV. Thus, in the European survey discussed above, more than 50 per cent of respondents agreed with the statement 'CCTV displaces[216] crime and does not protect against serious offences'.[217] A survey conducted on the Gold Coast in 2006 found that the public was sceptical about whether CCTV is effective without added measures.[218]

4.93 CCTV may create a perception of safety. For example, we learned in consultations that some homeless people in Victoria may derive a sense of safety from the presence of surveillance cameras.[219] We were also told about the use of CCTV to create a perception of safety in areas such as car parks, train stations and schools.[220]

4.94 In consultations the commission was told that the public has come to expect camera surveillance in certain settings. For example, it was suggested

182 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia* (2003) 13–15, noting that studies have produced mixed findings and citing Coretta Phillips, 'A Review of CCTV Evaluations: Crime reduction effects and attitudes towards its use' in Kate Painter and Nick Tilley (eds) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention* (1999); Brandon Welsh and David Farrington, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (2002); and Clive Coleman and Clive Norris, *Introducing Criminology* (2000).

183 Helene Wells et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 2.

184 Brandon Welsh and David Farrington, *Home Office Research Study 252 — Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (2002) i.

185 Brandon Welsh and David Farrington, 'Closed-Circuit Television Surveillance' in Brandon Welsh and David Farrington (eds) *Preventing Crime: What Works for Children, Offenders, Victims and Places* (2006) 193, 198.

186 Brandon Welsh and David Farrington, 'Closed-Circuit Television Surveillance' in Ibid 193, 198.

187 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) vi.

188 Ibid vi.

189 Ibid 61.

190 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia* (2003) 112.

191 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 4-5.

192 Ibid 78.

193 Ibid iii.

194 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 3.

195 Ibid 29-30; Brandon Welsh and David Farrington, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review* (2002) vii, 34–40.

196 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) vii and 33-40, 118.

197 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 2 (see studies cited therein).

198 ABC, 'Video Surveillance', *Catalyst,* 1 September 2005 <www.abc.net.au/catalyst/stories/s1450293.htm> at 21 January 2009.

199 Vanessa Goodwin, Crime Prevention and Community Safety Council [Tasmania], *Evaluation of the Devonport CCTV Scheme* (2002) 34.

200 Roundtable 6.

201 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia* (2003) 14.

202 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 5 (citation omitted).

203 Ibid 5–6.

204 See, eg, Kim McKay, *Better Policing Responses to Adult Sexual Assaults* 3 <www.aic.gov.au/conferences/2005-policewomen/mckay.pdf> at 30 June 2008; see also sentencing remarks in *R v Travis Rowland Agius* (SA District Court, 29 May 2008) <www.courts.sa.gov.au/sent_remarks/sr/0529_agius_travis_rowland.htm> at 30 June 2008.

205 See Justin Davenport, 'Tens of Thousands of CCTV Cameras, Yet 80% of Crime Unsolved' *Evening Standard* (London), 19 September 2007 <www.thisislondon.co.uk/news/article-23412867-details/Tens+of+thousands+of+CCTV+cameras,+yet+80%25+of+crime+unsolved/article.do> at 30 June 2008.

206 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 6.

207 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 65.

208 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 31-32.

209 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* A Report to the Criminology Research Council (CRC Grant 26/01-02) (2003) 109-110 [7.5]. See also Stephen Graham, et al, *Towns on the Television: Closed Circuit TV Surveillance in British Towns and Cities* (1995).

210 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia: A Comparative Study of Establishment and Operation* A Report to the Criminology Research Council (CRC Grant 26/01-02) (2003) 110.

211 Victorian Burglary Reduction Council, *How to Prevent your Shop from being Burgled* (date of publication unknown).

212 ABC, 'Video Surveillance', *Catalyst,* 1 September 2005 <www.abc.net.au/catalyst/stories/s1450293.htm> at 21 January 2009.

213 Interview with Mike Thompson, Linus Information Security Solutions (Telephone interview, 12 December 2008.

214 Roundtable 24.

215 Roundtable 22.

216 That is, moves it to other locations rather than reducing it in total

217 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 9.

218 Helene Wells, et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 47-49.

219 Roundtable 16.

220 Roundtable 2, 5, 7.

that people who have been assaulted on the tram are horrified if the tram does not have surveillance. More generally, it was suggested that when harmed people have an expectation that CCTV will capture the incident, and if a transport provider does not have CCTV it may be threatened with legal action.[221]

4.95 In some instances the demand for surveillance may outweigh concerns about the risks posed by surveillance practices. For example, in the transport roundtable the view was expressed that if an incident occurred the public would be less concerned about privacy and more about why an organisation does not have surveillance.[222] In our roundtable with government departments it was suggested that there is often public anger when images of an incident have not been captured through surveillance.[223]

4.96 In our roundtable with representatives from Indigenous justice bodies it was suggested that CCTV may provide protection against police aggression. It was suggested that CCTV ought to have the capacity to tilt and move to ensure that assaults by security guards and police do not escape the eye of the cameras.[224] The New South Wales Ombudsman has previously noted the role of CCTV as a source of evidence in complaints about incidents that occur in police custody, and that 'NSW Police have been working to improve the use of CCTV equipment and the availability and quality of the footage'.[225]

4.97 At least one study has concluded, however, that CCTV installation may not make people feel safer.[226] Moreover, creating a false sense of security carries its own risks, such as encouraging people to let down their guard. Finally, there is a question about whether merely creating a perception of safety is worth the cost of CCTV, with the annual operational costs of local government CCTV systems reported in 2003 to be $900,000 for Sydney and $400,000 for Melbourne.[227] There is also an opportunity cost associated with the inability to use more effective security measures because a CCTV system has consumed limited resources.

FREEDOM OF EXPRESSION AND JOURNALISTIC ACTIVITY

4.98 Surveillance is also used in public places to gather information for media stories. Changes to the way in which surveillance in public places is regulated may affect journalistic activities and, it may be argued, freedom of expression. [228]

4.99 Freedom of expression involves more than the right to express one's view. It includes the right to seek and receive information and ideas.[229] It has been suggested that it encompasses a right to seek, actively, generally available information.[230] For example, were security forces to take away a journalist's film of clashes between police and demonstrators, this would amount to an interference with the right to seek and receive information.[231]

4.100 While Australia does not have a Bill of Rights, the High Court of Australia has concluded that the Constitution contains an implied guarantee of freedom of communication about governmental and political matters.[232] Not all communication is protected, and the implied right is 'limited to what is necessary for the effective operation of that system of representative and responsible government provided for by the Constitution'.[233]

4.101 In Victoria, there is express mention of the right to freedom of expression in the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter). Section 15 of the Charter, which is modelled on the equivalent provision in the International Covenant of Civil and Political Rights (ICCPR), states:

> *(1) Every person has the right to hold an opinion without interference.*
> *(2) Every person has the right to freedom of expression which includes the freedom to seek, receive and impart information and ideas of all kinds, whether within or outside Victoria and whether—*
> *(a) orally; or*
> *(b) in writing; or*
> *(c) in print; or*
> *(d) by way of art; or*
> *(e) in another medium chosen by him or her.*

4.102 Like the right to privacy, the right to freedom of expression is not absolute. Section 15(3) of the Charter states that freedom of expression may be subject to lawful restrictions reasonably necessary:

> *a) to respect the rights and reputation of other persons; or*
> *b) for the protection of national security, public order, public health or public morality.*

4.103 Media organisations are always particularly concerned about any restrictions upon freedom of expression and it is widely accepted that an independent media, freely gathering and reporting on the news, is essential to a modern, democratic society. Eric Barendt has written:

> *the media provide readers, listeners, and viewers with information and that range of ideas and opinion which enables them to participate actively in a political democracy. Put shortly, the media perform a vital role as the "public watchdog". As the "eyes and ears of the general public" they investigate and report the abuse of power.*[234]

4.104 In recognition of the importance of gathering and publishing information in the public interest, national information privacy laws do not apply to the media.[235] The media are also exempt from information privacy laws in Canada, the UK, New Zealand and Hong Kong.[236] The exemption requires the media to engage in a considerable amount of self-regulation about privacy matters. [237]

4.105 Nevertheless, the media are subject to a range of laws which limit its ability to gather and report on news. For example, the tort of defamation restricts publication of information that damages the reputation of an individual.[238] National security laws and obscenity laws also restrict what the media can publish or broadcast.[239] Laws of general application, such as those concerned with trespass to land and interception of telephone calls, restrict the media's capacity to gather information prior to publication.

4.106 In addition, a number of statutes cause some court proceedings, such as those concerned with offences committed by children, to be closed to the public, thereby preventing media reporting.[240] In Victoria, section 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic) prohibits publication of the names of people subject to sexual assault.

4.107 Most media organisations are business enterprises that publish material for commercial purposes as well as to inform the community about important events. The Australian Privacy Foundation has highlighted that not all of the media's work is for 'public interest' purposes, and that one should distinguish genuine news and current affairs journalism from 'infotainment, entertainment and advertising'.[241]

4.108 It is harder for the media to claim a right to freedom of expression about matters published largely, or solely, for commercial reasons. For example, in the *Hannover* case, the European Court of Human Rights did not accept that photographs of Princess Caroline of Monaco when engaged in activities such as shopping and practising sport did more than minimally engage the right to freedom of expression. According to the Court, the photographs did not contribute to any debate of general interest to society, but were intended merely to satisfy the curiosity of readers about the Princess's private life.[242]

4.109 Similarly, the UK House of Lords concluded that the media's need to disseminate photographs of model Naomi Campbell leaving a Narcotics Anonymous meeting was a form of expression that was of lesser value than the need to disseminate information on other subjects, such as political information.[243] More recently, an English High Court judge found that a newspaper's reports about the private sexual activities of celebrity Max Mosley were not published in the public interest.[244]

221 Roundtable 19.

222 Roundtable 19.

223 Roundtable 1.

224 Roundtable 28.

225 NSW Ombudsman, *Annual Report 2003–2004* (2004) 123.

226 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 60–1.

227 Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia* (2003) 71, <www.criminologyresearchcouncil.gov.au/reports/200102-26.pdf> at 16 January 2009.

228 See eg, *Campbell v MGN Limited* [2004] UKHL 22, [55] (Lord Hoffman).

229 *Universal Declaration of Human Rights* GA res 217A (III), UN GAOR, 3rd sess, UN doc A/810 at 71 (1948) art19.

230 Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (2nd revised ed) (2005) 446–7.

231 Ibid 447.

232 *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 163; and *Lange v Australian Broadcast Corporation* (1997) 189 CLR 520, 560–1.

233 *Lange v Australian Broadcast Corporation* (1997) 189 CLR 520, 561.

234 Eric Barendt, *Freedom of Speech* (2nd ed) (2005) 417–418 (footnotes omitted).

235 *Privacy Act 1988* (Cth) s 7B(4). See generally Ch 5 for further discussion of information privacy laws and media codes.

236 *Privacy Act*, RS C 1980, c P-21, s 69.1 [Canada]; *Data Protection Act 1998* [UK] c 29, s 32; Privacy Act 1993 [NZ] s 2(1)(b)(xiii); *Personal Data (Privacy) Ordinance 1995* [HK] s 61.

237 The commission notes that The Media Alliance Code of Ethics includes a direction to Alliance members engaged in journalism to 'commit themselves to … respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude': Media Entertainment and Arts Alliance, *Media Alliance Code of Ethics* (1999) <http://www.alliance.org.au/resources/media/> at 12 February 2009.

238 See eg, *Defamation Act 2005* (Vic).

239 *National Security Information (Criminal Proceedings) Act* 2004 (Cth) and *Summary Offences Act 1966* (Vic).

240 For example, s 107(1) of the *Adoption Act 1984* (Vic) requires applications for adoption to be heard in a closed court. Likewise, s 47 of the *Coroners Act 1985* (Vic) allows a coroner to exclude individuals from an inquest. See Australia's Right to Know Coalition, *Report of the Independent Audit into the State of Free Speech in Australia* (2007) for a review of legislation in other states having the same effect.

241 Australian Privacy Foundation, *'Australia's Right to Know' Coalition: Independent Audit into the State of Media Freedom in Australia* (APF submission, August 2007) 4.

242 *Von Hannover v Germany* (2004) VI Eur Court HR 294, [65].

243 *Campbell v MGN Limited* [2004] UKHL 22, [29].

244 Mosley v News Group Newspapers Ltd [2008] EWHC 1777 (QB) (Eady J) [16] citing Press Complaints Commission, *Press Complaints Commission Code of Practice* (2007) cl 10 <www.pcc.org.uk/cop/practice.html> at 15 January 2009.

Chapter 4 Risks and Benefits

4.110 David Morrison and Michael Svennevig have noted that what is in public interest is not the same as what interests the public.[245] Not all things of 'news value' are in the public interest, and the converse is true.[246]

4.111 A number of law reform commissions have recognised the importance of distinguishing between the media's right to free expression about matters of public interest and about matters of mere news value. For example, the Irish Law Reform Commission in its report on surveillance said:

> *the public interest secured by the people's right to know a particular piece of information is not synonymous with whatever happens to interest the public. Mere newsworthiness is not a reliable proxy for the public interest…The exposure of true facts does not, in our view, have any absolute value.*[247]

Similarly, the ALRC's recent recommendation that the exemption for the media under the *Privacy Act 1988* (Cth) apply only to media activities meeting a newly proposed definition of 'journalism'[248] recognises that not all journalistic activities are of equal value to the community.

4.112 In the United States, the courts generally treat media reports about political matters and light 'entertainment' in the same way[249] permitting the media to publish what it has considered 'newsworthy'.[250] In addition, courts in the US have been reluctant to distinguish between speech about 'true' public figures such as politicians, and about private figures cast into the public spotlight. For example, the California Court of Appeal concluded in 1984 that there was a public interest in the media reporting that a man who had thwarted an assassination attempt on former US President Gerald Ford was gay.[251] It has been suggested that once a person has intentionally or unintentionally done something notable under US law, their life is subject to scrutiny.[252]

4.113 The alleged benefit of the US approach is that it overcomes the difficulty of distinguishing between speech of a 'public interest' nature and speech that does not have that value.[253] As Morrison and Svennevig argue, the notion of a 'public interest' assumes both a consensus about what falls within this concept and a capacity within some person or group to determine that consensus.[254] Commentators have also suggested that information about celebrities' lives may serve a social function, because people can model their lives on those of the celebrities.[255] For example, a German court reasoned in the case that subsequently became the *Hannover* case at the European Court of Human Rights concerning Princess Caroline of Monaco that:

> *Entertaining articles can also contribute to the formation of opinions. Such articles can, under certain circumstances, stimulate or influence the formation of opinions in a more sustainable way than information that is exclusively fact-related… Moreover, prominent persons also stand for certain ethical positions and views of life.*[256]

4.114 Finally, private citizens increasingly use various forms of public place surveillance for journalistic purposes. For example, cameras are often used to further social or political action by recording activities in public places. We have also previously referred to the phenomenon of 'snapperazzi': amateurs with mobile phones who follow celebrities and sell photographs of them to the magazines.[257]

4.115 Such citizen journalism, in addition to being an exercise of freedom of expression, suggests a possible democratising effect of surveillance. The dissemination of surveillance technologies throughout society (a phenomenon called the 'synopticon', in contrast to the panopticon) challenges the notion that surveillance is no more than an instrument of social control. Rather, the widespread use of surveillance devices means that citizens can 'scrutinize the demeanour, foibles and idiosyncrasies of powerful individuals to an entirely unprecedented extent'.[258]

CONCLUSION

4.116 Public place surveillance offers both benefits and risks. Do the risks outweigh the benefits? The answer depends on a range of matters including the type of public place surveillance under consideration, the purpose for which it is used, and the identity of the organisation or person conducting the surveillance.

4.117 Achieving a balance between the risks and benefits of public place surveillance almost certainly involves personal choice as well as regulation. As individuals, we are sometimes presented with a choice about whether to forfeit some aspects of our privacy in exchange for one or more of the benefits of public place surveillance. For example, some people may be willing to give up privacy with respect to their car travel patterns in return for speedier travel on a toll road. But is this free choice? During the current trial phase of the x-ray body scanners at Melbourne airport, people will be able to decide whether to trade away privacy with respect to their body image to avoid submitting to the alternative, a physical pat-down.[259]

4.118 As these examples suggest, however, the notion of choice may sometimes be illusory. The non-toll roads may be heavily congested, and the alternative of a pat-down search may not be any less privacy invasive than a full body scan. Moreover, as public place surveillance becomes more widespread, we may find ourselves trading away privacy not merely for convenience, but in order to access basic services.

245 David Morrison and Michael Svennevig, 'The Defence of Public Interest and the Intrusion of Privacy' (2007) 8 (1) *Journalism* 44, 44.

246 Ibid 49.

247 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [1.59]–[1.60].

248 Australian Law Reform Commission, *Review of Australian Privacy Law: Volume 2: Discussion Paper* Discussion Paper 72 (2007) vol 2, Discussion Paper 72, Proposal 38–1, 1099–1100.

249 Eric Barendt, 'Privacy and Freedom of Speech' in Andrew Kenyon and Megan Richardson (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives* (2006) 11, 20.

250 Camrin Crisci, 'All the World is Not a Stage: Finding a Rights to Privacy in Existing and Proposed Legislation' (2002) 6 *New York University Journal of Legislation and Public Policy* 207, 219–20. See also the *Restatements*, which say that 'To a considerable extent, in accordance with the mores of the community, the publishers and broadcasters have themselves defined the term [news]' American Law Institute, *Restatement of the Law Second, Torts* (1965) § 652D comment (g).

251 *Sipple v Chronicle Publishing Co* (1984) 154 Cal App 3d 1040, 1048–50.

252 Camrin Crisci, 'All the World is Not a Stage: Finding a Rights to Privacy in Existing and Proposed Legislation' (2002) 6 *New York University Journal of Legislation and Public Policy* 207, 225.

253 David Morrison and Michael Svennevig, 'The Defence of Public Interest and the Intrusion of Privacy' (2007) 8 (1) *Journalism* 44, 55.

254 Ibid 48.

255 See Richard Posner, 'The Right of Privacy' (1978) 12 (3) *Georgia Law Review* 393, 396; Camrin Crisci, 'All the World is Not a Stage: Finding a Rights to Privacy in Existing and Proposed Legislation' (2002) 6 *New York University Journal of Legislation and Public Policy* 207, 217.

256 Federal Constitutional Court (Bundesverfassungsgericht) [Germany] *In the Proceedings of the Constitutional Complaint of Princess Caroline of Monaco*, 15 December 1999 (1999) 1 BvR 653/96.

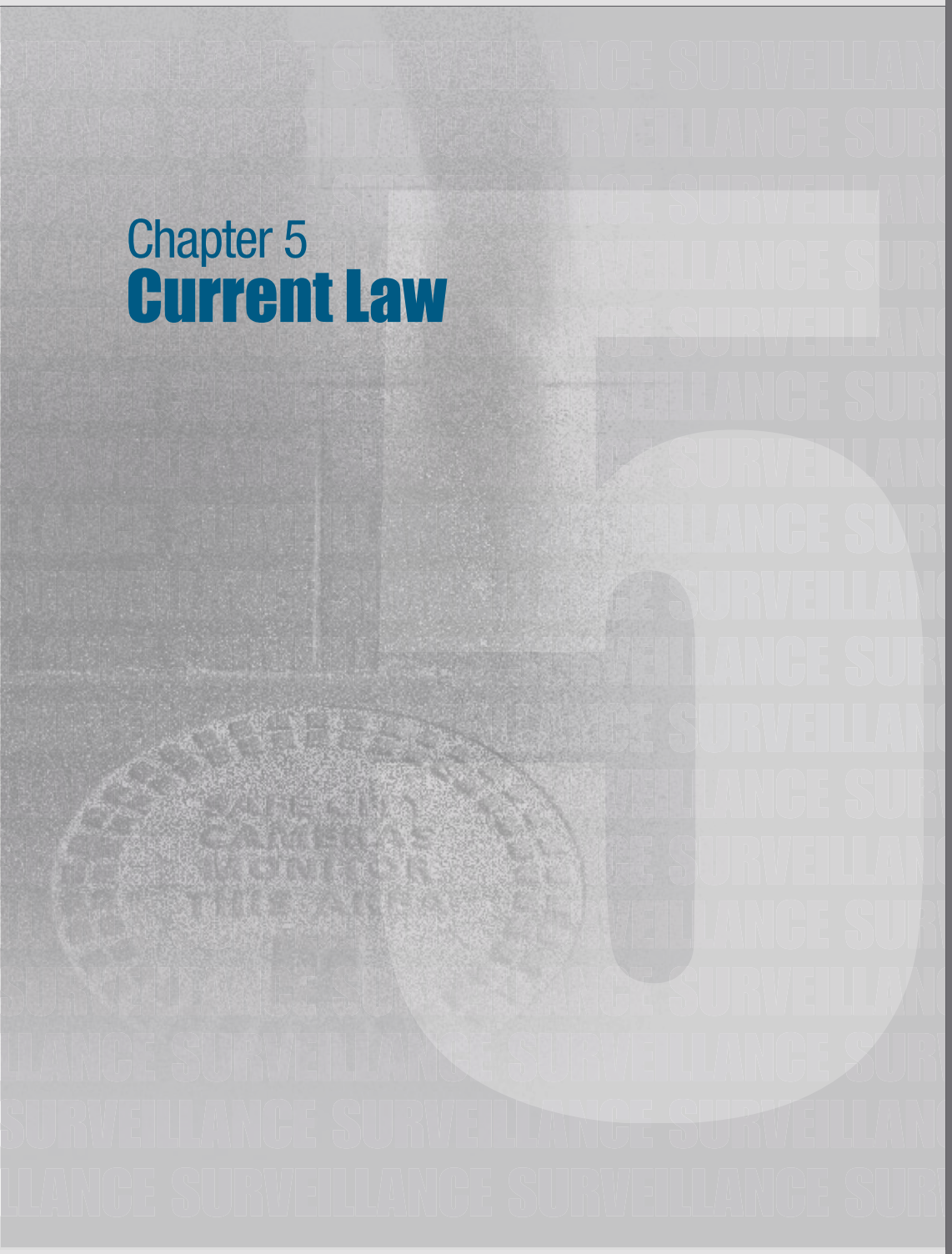
257 Steve Dow, 'The Power of the Citizen Paparazzi', *The Sun Herald* (Sydney), 30 January 2005, 78.

258 Kevin Haggerty, 'Tear Down the Walls: On Demolishing the Panopticon' in Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 (4) *British Journal of Sociology* 605;David Lyon (ed) *Theorizing Surveillance: The Panopticon and Beyond* (2006) 30.

259 Dan Oakes, 'Melbourne Airport Scanners "Will Show Private Parts"', *Sydney Morning Herald* (Sydney), 15 October 2008 <www.smh.com.au/news/news/airport-scanners-show-genitals/2008/10/15/1223750083412.html> at 21 January 2009.

Chapter4

Risks and Benefits



Chapter 5
Current Law

Chapter 5

Current Law

INTRODUCTION

5.1 In this chapter we describe how surveillance in public places is regulated in Victoria. The chapter begins with an overview of the relevant law before moving to a detailed consideration of specific laws, guidelines and policies that govern particular activities and practices. We also discuss laws relating to surveillance practices in other Australian jurisdictions and in other countries.

OVERVIEW OF THE LAW

5.2 There are two main bodies of law concerning surveillance in public places in Victoria—the *Surveillance Devices Act 1999* (Vic) (SDA (Vic)) and the Commonwealth and Victorian laws that regulate the privacy of personal information.[1] Currently surveillance activities in public places are not illegal unless prohibited by these laws, or regulated by some other specific laws that apply to particular industries.

5.3 The SDA (Vic) prohibits some surveillance activities in public places. The Act regulates the use of four types of surveillance devices—listening devices, optical surveillance devices, tracking devices and data surveillance devices. The level of protection provided by the Act in public places differs according to the type of device used and surveillance activity undertaken. For example, a person is prohibited from using a listening device to monitor a private conversation without consent indoors and outdoors. By contrast, a person is prohibited from using an optical surveillance device to monitor a private activity without consent indoors, but there is no prohibition on the use of optical surveillance devices outdoors. Breaches of the Act attract criminal sanctions. Victorian police and other law enforcement officers may use surveillance devices in ways otherwise prohibited by the Act if they obtain a warrant from a judge or magistrate.

5.4 Surveillance users may also be subject to Victorian and Commonwealth information privacy laws that regulate the handling of 'personal information'[2] because at least some forms of surveillance will result in the collection and use of personal information. Personal information is defined in those laws as information that is recorded and that concerns an individual whose identity is apparent, or can be reasonably ascertained, from the information.[3]

5.5 Under the information privacy laws, personal information must be collected by lawful and fair means, and used only for the primary purpose for which it was collected. The laws also contain other privacy principles relating to the use, disclosure, retention and disposal of personal information after collection. Breaches of information privacy laws can result in orders for compensatory damages.

5.6 A number of other laws also regulate public place surveillance. For example, the use of surveillance devices is expressly permitted in particular industries, such as taxis and casinos. There are also laws that prohibit particular types of surveillance activities, for example those associated with stalking[4] or the practice of 'upskirting' in which a device such as a camera is secretly held under a person's clothing to view that person's intimate areas.[5]

5.7 Some surveillance practices—such as monitoring telecommunications—are prohibited except when performed by nominated people, such as law enforcement officers, authorised by warrant. Tables 1 and 2 on page 126-129 contain an overview of the legislation and major non-binding instruments relating to the regulation of public place surveillance in Victoria.

5.8 The extent to which the common law may develop to regulate the use of surveillance in public places is unclear. In other countries, a tort of privacy or an equitable duty of confidence provides some protection against interference with seclusion and/or the misuse of private information obtained by surveillance activities. In Australia, the High Court has not yet recognised a common law right to privacy, although there have been developments in lower courts. Trial courts in Victoria and Queensland have recognised a right to privacy and awarded damages to compensate for invasion of that right. Those cases decided that privacy intrusion was unlawful when it 'would be considered highly offensive to a reasonable person of ordinary sensibilities.'[6] In Victoria, the Court of Appeal has recently

decided that damages may be awarded for breach of the duty of confidence.[7] While this decision makes the cause of action more attractive to people who have suffered harm because of the misuse of sensitive personal information, the precise boundaries of the duty of confidence are difficult to identify, particularly when the information is misused by a stranger.

SURVEILLANCE LEGISLATION

VICTORIA

Background

5.9 The first surveillance device legislation in Victoria, the *Listening Devices Act 1969* (Vic) (Listening Devices Act), was enacted to protect the privacy of private conversations.[8] The Act prohibited the non-consensual use of listening devices to record 'private conversations'[9] which were those which could not reasonably be expected to be overheard by others.[10] The Act also prohibited the publication of records or reports of private conversations, except in limited circumstances.[11]

5.10 In 1999 the SDA (Vic) was enacted to replace the Listening Devices Act because of advances in technology. One of the primary concerns was inappropriate use of video cameras. The new legislation extended the existing controls concerning listening devices by regulating three additional types of surveillance devices: optical surveillance devices, tracking devices and data surveillance devices.[12] In the second reading speech, the Attorney-General said that the SDA (Vic) was designed to provide 'stringent safeguards to protect individual privacy'.[13] The Shadow Attorney General supported the Bill, noting 'the improvement in technology over the years makes the present legislation, the Listening Devices Act, redundant'.[14]

Application to public place surveillance

5.11 The extent to which listening, optical, tracking and data surveillance devices may lawfully be used under the SDA (Vic) differs according to the type of device and the activity undertaken. For example, the Act prohibits the use of a listening device to monitor a 'private conversation' anywhere, while it only prohibits the use of an optical surveillance device to monitor a 'private activity' indoors.[15] Further, unlike prohibitions on the use of listening or optical surveillance devices, prohibitions on the use of tracking and data surveillance devices apply whether or not there is a private aspect to the information being monitored.[16] Thus, under the Act:

- A person may use a listening device (such as a tape recorder) to record conversations in an indoor or outdoor public place, except where it involves a private conversation, in which case consent must be sought.
- A person may use an optical surveillance device (such as closed-circuit television (CCTV), video camera or still-photo camera) in an indoor public place for surveillance purposes except where it involves a private activity. Consent from the person under surveillance is required to record a private activity.[17] In contrast, a person may film any activity, private or otherwise, outdoors, without consent.
- A person is prohibited from tracking a person's movements without consent. In order to track an object (for example, a car), consent from the owner must be obtained. This prohibition is limited only to devices with a primary purpose of tracking (for example, a car's satellite navigational device, not a mobile telephone with global positioning system (GPS) capabilities).
- A person is able to use a data surveillance device[18] (for example spyware) and to lawfully communicate and publish information obtained regardless of whether the information is private or consent is sought. Only law enforcement officers are prohibited from communicating or publishing information obtained from a data surveillance device unless consent is sought or some other exception applies.[19] As outlined in Chapter 1, surveillance conducted through a data surveillance device is outside the scope of this inquiry.

1 *Privacy Act 1988* (Cth), *Information Privacy Act 2000* (Vic). The *Privacy Act 1988* (Cth) (Privacy Act) regulates the practices of Commonwealth government agencies and some private sector organisations, and the *Information Privacy Act 2000* (Vic) (IPA) regulates the practices of Victorian government agencies.

2 Ibid.

3 Personal information is defined in the *Privacy Act 1988* (Cth) s 6 (read in conjunction with section 16B), and the *Information Privacy Act 2000* (Vic) s 3.

4 *Crimes Act 1958* (Vic) s 21A.

5 *Summary Offences Act 1966* (Vic) div 4A.

6 *Grosse v Purvis* [2003] QDC 151 is discussed later in this chapter in the section titled 'Invasion of privacy: An emerging cause of action'.

7 *Giller v Procopets* [2008] VSCA 236.

8 It was described as 'primarily actuated by the desire that the individual man or woman should be protected against persons who spy on his or her private conversations': see Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 546 (Rob Hulls).

9 *Listening Devices Act 1969* (Vic) s 4(1).

10 *Listening Devices Act 1969* (Vic) s 3.

11 Such limited circumstances included where the communication or publication was 'no more than is reasonably necessary in the public interest or in the course of [a person's] duty or for the protection of his [or her] lawful interests'. *Listening Devices Act 1969* (Vic) s 4(2).

12 These terms are defined in the *Surveillance Devices Act 1999* (Vic) s 3(1).

13 Victoria, *Parliamentary Debates*, Legislative Assembly, 25 March 1999, 192 (Jan Wade).

14 Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 546 (Rob Hulls).

15 This is because the Act's definitions of 'private activity' and 'private conversation' are not consistent. While a private conversation may occur anywhere, a private activity may only occur indoors. See *Surveillance Devices Act 1999* (Vic) s 3.

16 *Surveillance Devices Act 1999* (Vic) ss 8 and 9.

17 In the case of tracking devices, without the express or implied consent of the person who lawfully possesses or controls the object being tracked: *Surveillance Devices Act 1999* (Vic) s 8(1)(b).

18 *Surveillance Devices Act 1999* (Vic) s 3(1): a data surveillance device is a device that can be used to record or monitor the input or output of information in a computer.

19 *Surveillance Devices Act 1999* (Vic) s 12.

Chapter 5 Current Law

5.12 Surveillance activities that are not prohibited by the SDA (Vic), or any other law, are permissible. The SDA (Vic) does not prohibit many forms of surveillance that occur in public places. These include:

- optical surveillance outside a building
- optical surveillance in an indoor shopping mall (other than in enclosed spaces such as toilet cubicles and change rooms)
- audio surveillance in busy outdoor and indoor areas, unless it involves recording hushed conversations
- tracking movement with devices which have a primary purpose other than tracking (such as mobile phones)
- surveillance without the use of a device (such as private investigator surveillance)[20]
- secretly recording a conversation or activity to which one is a party.

5.13 The SDA (Vic) also regulates the use of information gathered by a surveillance device. A person may lawfully communicate and publish information obtained from a listening, optical surveillance, or tracking device unless it involves a private conversation or activity.[21] Private information obtained in these circumstances may be published only when consent has been given or some other express exclusion applies, such as disclosure that is in the public interest, or where there is a law enforcement exception.[22]

Limitations

'Private conversations' and 'private activities'

5.14 The prohibitions in the SDA (Vic) concerning the use of listening and optical surveillance devices are limited to 'private conversations' and 'private activities', respectively.

5.15 A *'private conversation'* is one carried on in circumstances that reasonably indicate that the parties 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'.[23]

5.16 Many conversations occur in public places in circumstances where it is reasonable for the participants to expect that they will be overheard. It is also reasonable to expect, however, that some conversations in less frequented places, such as quiet parks and beaches, will not be overheard. These conversations are covered by the Act and may not be monitored or recorded unless they fall within the law enforcement exception.

5.17 Whether an exchange is a private conversation will depend on the particular circumstances. Decisions under similar regulatory regimes provide some guidance. For example, a conversation in an office with the door open was treated as a private conversation even though it might conceivably have been overheard by a passer-by.[24] By contrast, a conversation in the open floor area of retail premises failed to qualify as private.[25] During parliamentary debate about the SDA (Vic), a number of members considered the possibility that hushed conversations in restaurants would constitute 'private conversations' under the Act.[26]

5.18 A *'private activity'* is one that is carried on inside a building and in circumstances that reasonably indicate the parties desire it be observed only by themselves and where they may reasonably expect that they will not be observed by someone else.[27] Thus, the SDA (Vic) offers no protection against unwanted visual surveillance in outdoor public places. During the debate prior to the enactment of the SDA (Vic), a number of parliamentarians referred to this lack of protection provided to private activities in outdoor places, such as beaches and backyards.[28] This issue has recently generated community interest, sparked by the satellite images and photographs published by Google Street View and used by some NSW and Victorian councils.[29] In 2005, the Federation of Parents and Citizens Associations responded to concern about pornographic use of photographs taken of children in public by suggesting that parents should have to gain permission from schools to film or photograph their child at swimming carnivals, school plays and other events.[30]

5.19 The SDA (Vic)'s prohibition on the use of an optical surveillance device to observe or record

a 'private activity' clearly includes activities in very private areas of public facilities, such as toilet cubicles and enclosed showers.[31] It is not clear, however, whether this prohibition extends to open shower areas, change rooms, and even male urinals, since a person must reasonably expect to be seen by others when using these communal facilities.[32] This lack of clarity is evidenced by the fact that some gyms have instituted their own policies banning the use of mobile telephones in areas of this nature. The Victorian Privacy Commissioner has queried whether the SDA (Vic) provides sufficient privacy protection for activities that occur in those parts of change rooms where individuals may be seen by others.[33]

Regulation limited to defined devices

5.20 As discussed above, the SDA (Vic) regulates practices involving four specific types of surveillance devices: listening devices, optical surveillance devices, tracking devices and data surveillance devices. Further, the level of protection provided by the Act differs according to the type of device used. Any surveillance that occurs without the involvement of one of these devices is not regulated by the Act. The fact that the SDA (Vic) places different restrictions on different devices has the potential to create confusion because widely used modern technology, such as mobile phones, can perform a number of surveillance functions.

Does not apply to a party to a private conversation or activity

5.21 The prohibitions in the SDA (Vic) concerning the use of listening devices and optical surveillance devices do not extend to a person who uses one of those devices to record a conversation or activity to which they are party. This is known as 'participant monitoring'. The SDA (Vic) permits a person who is party to a conversation or activity to record that conversation or activity without the knowledge or consent of the other people involved. The SDA (Vic) does prohibit a person from knowingly communicating or publishing a record of a private conversation or activity in which that person participated without the consent of other participants. There are broad exceptions to that prohibition.[34]

Regulation of tracking device limited to 'primary use' of device

5.22 The SDA (Vic) regulates the use of a tracking device if the device in question is 'an electronic device the primary purpose of which is to determine the geographical location of a person or an object'.[35] This means that devices which are capable of tracking but which have another primary purpose, such as mobile phones with GPS capabilities, are not regulated by the Act.

A lack of guidance relating to the requirement of consent

5.23 The SDA (Vic) does not apply to the use of devices where the person monitored has consented to this action.[36] The relevant sections in the Act refer to the 'express or implied consent' of the person concerned. While the notion of express consent appears to raise few difficulties, implied consent is more problematic. Do clear signs that notify people of the existence of some form of surveillance—such as CCTV cameras—in a particular area, mean that all people who enter the area have given implied consent to their activities being monitored and recorded? Is any implied 'consent' truly voluntary if the subject of surveillance has no reasonable opportunity to 'opt out'? Problems associated with the notion of implied consent were raised by the Australian Law Reform Commission (ALRC) in the context of information privacy laws.[37] The commission recommended that the Federal Privacy Commissioner provide further guidance on the meaning of consent, including the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained.[38]

20 However, a number of other Acts prohibit certain forms of behaviour relating to personal surveillance; for example, the *Crimes Act 1958* (Vic) s 21A prohibits stalking.

21 *Surveillance Devices Act 1999* (Vic) s 11.

22 *Surveillance Devices Act 1999* (Vic) s 11.

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

24 See *Miller v TCN Channel Nine* (1988) 36 A Crim R 92, 106.

25 *Steiner Wildon and Webster Pty Ltd v Amalgamated Television Services Pty Ltd* [2000] Aust Torts Reports 81-537 [322].

26 Victoria, *Parliamentary Debates*, Legislative Council, 11 May 1999, 525 (Maree Luckins) stating 'private conversations which take place inside a restaurant are protected, but those undertaken outside will not be afforded the same protection'; see also Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 556 (Victor Perton) querying whether the Act would prohibit surveillance of business or political discussions in restaurants where people 'do not expect to be overheard in those conversations'.

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

28 Victoria, *Parliamentary Debates,* Legislative Council, 11 May 1999, 524–525 (Maree Luckins); Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 551 (Robert Hulls), 555 (Victor Perton), 559 (Hurtle Lupton).

29 Roundtable 10 and Asher Moses, 'Anyone for a Gentle Google Down Wisteria Lane?', *The Age* (Melbourne), 6 August 2008, 5. See discussion in Chapter 2.

30 Lisa Carapiet, 'Sign here to take that Poolside Snap', *Sydney Morning Herald* (Sydney) 22 February 2005 <www.smh.com.au/news/National/Sign-here-to-take-that-poolside-snap/2005/02/21/1108834734922.html> at 5 January 2009.

31 Explanatory Memorandum, Surveillance Devices Bill 1999 (Vic) cl 3.

32 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003) 4.

33 Ibid.

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

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

36 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1).

37 This is discussed later in this chapter when we consider information privacy laws.

38 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) 684 and 686 (Recommendation 19–1).

Chapter 5 Current Law

Gaps in the regulation of law enforcement

5.24 While surveillance undertaken for law enforcement purposes is not within the ambit of this inquiry, it is useful to outline some of the major limitations of surveillance devices legislation in relation to law enforcement activities. Victorian police and other law enforcement officers may use surveillance devices in ways that are prohibited by the Act if they obtain a warrant from a judge or magistrate,[39] and in other limited circumstances. For example, under the *Surveillance Devices Act 2004* (Cth) (SDA (Cth)), a federal law enforcement officer does not need a warrant to use an optical surveillance device in circumstances where he or she does not enter premises or interfere with a vehicle without consent.[40] A federal officer also does not need a warrant to use a listening device to record a conversation to which he or she is a party,[41] and any law enforcement officer only needs the permission of a senior officer to use a tracking device in the investigation of a federal offence.[42] Under the SDA (Vic), surveillance for law enforcement purposes without a warrant is permitted in limited circumstances, including where it is carried out in accordance with a Commonwealth law;[43] and, in relation to listening and optical surveillance devices, where the officer reasonably believes it is necessary for the protection of any person's safety, and has the consent of a required party.[44]

5.25 The warrant procedures in the SDA (Vic) do not protect the privacy of innocent third parties who may be caught up in an investigation where surveillance is used. For example, there is no requirement for courts to make orders concerning measures to delete or de-identify images and conversations of third parties that are not required for the purposes of the investigation, or as evidence in any court proceedings. There is also lack of transparency about the issuing of warrants. In contrast to the position under the SDA (Cth), there is no published information about warrants granted under the SDA (Vic).

Enforcement

5.26 It is a criminal offence to breach the prohibitions in the SDA (Vic) concerning the use of surveillance devices. The maximum penalties are severe. A person who contravenes sections 6, 7, 8, or 11 of the Act[45] is liable to a maximum penalty of two years imprisonment and/or 240 penalty units (currently $27,220).[46] A corporation is liable to a maximum penalty of 1200 penalty units (currently $136,104). There is no formal mechanism for individuals to make a complaint about violations of the Act, nor a right to bring a civil action for damages in response to breaches of the Act.

5.27 No organisation or agency has a specific responsibility for monitoring compliance with the provisions of the SDA (Vic), or for providing public education about the privacy implications of surveillance practices. Because the SDA (Vic) contains criminal offences, Victoria Police has a general responsibility to act in response to suspected or reported breaches of the Act. The commission is not aware of any police prosecutions for violations of the SDA (Vic).

5.28 Further, no organisation or agency has responsibility for monitoring the use of surveillance in public places and for receiving complaints from members of the community who are concerned about surveillance activities. In some other countries Privacy and Data Protection Commissioners have responsibility for overseeing various aspects of public surveillance, such as the use of some types of CCTV camera systems.[47]

Exclusions

5.29 The SDA (Vic) does not apply to the Australian Federal Police and other Commonwealth agencies.[48] The activities of Commonwealth law enforcement officers are regulated by the SDA (Cth). That Act establishes procedures for law enforcement officers to obtain warrants for offences against a Commonwealth law (or a state law that has a federal aspect) punishable by a maximum term of imprisonment of three years or more.[49]

5.30 Other agencies whose uses of surveillance devices are specifically excluded from the operation of the SDA (Vic) and therefore legal in Victoria unless they breach other laws (such as the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) or laws of trespass) are:

- the Australian Competition and Consumer Commission[50]
- the Australian Security Intelligence Organisation[51]
- the Australian Federal Police, except for officers acting in their capacity as a member of staff of the Australian Crime Commission[52]
- customs officers within the meaning of the *Customs Act 1901* (Cth)[53]
- migration officers and employees acting under the *Migration Act 1958* (Cth).[54]

5.31 Also excluded are agencies acting in accordance with Commonwealth laws which permit the use of surveillance devices.[55] The bodies which may use surveillance devices in Victoria include the Australian Commission for Law Enforcement Integrity[56] and various state police and integrity bodies[57] (as well as to the Australian Federal Police and the Australian Crime Commission).

OTHER AUSTRALIAN JURISDICTIONS

5.32 All Australian states and territories have legislation that regulates the use of surveillance devices, although in some jurisdictions only the use of listening devices is covered.[58] Victoria, New South Wales, the Northern Territory, South Australia and Western Australia have laws which extend to devices other than listening devices.[59]

5.33 The *Surveillance Devices Act 2007* (NSW) (SDA (NSW)) merits close consideration because it has only recently become law. While that Act regulates the same types of surveillance devices as the SDA (Vic), there are number of key differences in the way this is done. For example, the regulation of optical surveillance devices is quite different. Under the SDA (NSW), it is unlawful to use an optical surveillance device to observe or record *any* activity (not only private activities), but only where it involves entry into a building or vehicle without consent, or interference with a vehicle or other object without consent.[60]

5.34 Unlike the Victorian Act, the SDA (NSW) prohibits the use of a listening device without the consent of all parties to the conversation.[61] Thus, unlike the SDA (Vic), the SDA (NSW) prohibits 'participant monitoring' or recording a private conversation by a person who is a party to the conversation. The NSW prohibition against tracking devices[62] also offers stronger protection than the Victorian legislation because it includes devices not primarily intended for tracking.[63]

5.35 The SDA (NSW) also contains an offence in relation to possession of information obtained from the illegal use of a surveillance device,[64] and it outlaws the manufacture, supply or possession of surveillance devices for unlawful use.[65]

5.36 Some other states also have more extensive restrictions upon the use surveillance devices than Victoria. For example:

- Participant monitoring of a conversation using a listening device is prohibited in the Australian Capital Territory, Western Australia, Tasmania and South Australia;[66] participant monitoring of a private activity using an optical surveillance device is prohibited in Western Australia.[67]
- The use of an optical surveillance device to monitor a private activity which occurs outdoors is prohibited in Western Australia and the Northern Territory, provided it is not an activity the parties ought reasonably to expect may be observed.[68]

39 *Surveillance Devices Act 1999* (Vic) pt 4.

40 *Surveillance Devices Act 2004* (Cth) s 37(1).

41 *Surveillance Devices Act 2004* (Cth) s 38(1).

42 *Surveillance Devices Act 2004* (Cth) s 39(1).

43 *Surveillance Devices Act 1999* (Vic) ss 6(2)(b), 7(2)(b), 8(2)(b) and 9(2)(b).

44 *Surveillance Devices Act 1999* (Vic) ss 6(2)(c), 7(2)(c).

45 Regulating the use and maintenance of the four types of surveillance devices, and prohibiting the communication and publication of private conversations or activities.

46 *Surveillance Devices Act 1999* (Vic) ss 6, 7, 8. In the case of the prohibition on law enforcement use of a data surveillance device, a maximum penalty of one year imprisonment and/or 120 penalty units: *Surveillance Devices Act 1999* (Vic) s 9.

47 We discuss surveillance regulation in other countries later in this Chapter.

48 *Surveillance Devices Act 1999* (Vic) s 5.

49 *Surveillance Devices Act 2004* (Cth) s 6 (definition of 'relevant offence').

50 The Australian Competition and Consumer Commission derives its investigative powers from the *Trade Practices Act 1974* (Cth) pt XID.

51 ASIO has broad investigative powers under Part III of the *Australian Security Intelligence Organisation Act 1979* (Cth).

52 The general powers and functions of AFP are set out in the *Australian Federal Police Act 1979* (Cth) while their use of surveillance devices is regulated via the *Surveillance Devices Act 2004* (Cth).

53 The *Customs Act 1901* (Cth) contains some investigative powers in pt XII, sub-div B.

54 The *Migration Act 1958* (Cth) contains a number of investigative powers in pt 2 divs 12A, 13 and 14A including a power in s 268CI to take photographs or make video or audio recordings.

55 The key Commonwealth law regulating surveillance devices is the *Surveillance Devices Act 2004* (Cth).

56 The Australian Commission for Law Enforcement Integrity derives investigative powers from the *Law Enforcement Integrity Commissioner Act 2006* (Cth) pt 9.

57 These are the police force of each State or Territory, the NSW Crime Commission, the Queensland Crime and the Western Australian Misconduct Commission and the Corruption and Crime Commission: see definition of 'law enforcement agency' in the *Surveillance Devices Act 2004* (Cth) s 6(1).

58 See *Listening Devices Act 1992 (*ACT); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1991* (Tas).

59 *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Listening and Surveillance Devices Act 1972* (SA); *Surveillance Devices Act 1998* (WA).

60 *Surveillance Devices Act 2007* (NSW) s 8.

61 *Surveillance Devices Act 2007* (NSW) s 7.

62 See *Surveillance Devices Act 2007* (NSW) s 9.

63 See *Surveillance Devices Act 2007* (NSW) s 4(1).

64 *Surveillance Devices Act 2007* (NSW) s 12.

65 *Surveillance Devices Act 2007* (NSW) s 13.

66 See *Listening Devices Act 1992 (*ACT) s 4(1)(b); *Surveillance Devices Act 1998* (WA) s 5(1)(b); *Listening Devices Act 1991* (Tas) s 5(1)(b); *Listening and Surveillance Devices Act 1972* (SA) s 4.

67 *Surveillance Devices Act 1998* (WA) s 6(1)(b).

68 See *Re Surveillance Devices Act 1998: Ex Parte TCN Channel Nine Pty Ltd* [1999] WASC 246; *Surveillance Devices Act 2007* (NT) ss 4 and 12.

Chapter 5 Current Law

INFORMATION PRIVACY LEGISLATION

VICTORIA AND THE COMMONWEALTH

5.37 Commonwealth and Victorian information privacy laws regulate the handling of 'personal information'.[69] The *Privacy Act 1988* (Cth) (Privacy Act (Cth)) contains a set of Information Privacy Principles (IPPs)[70] that govern the collection, storage and use of 'personal information' by Commonwealth government agencies.[71] It also regulates the information privacy practices of private sector organisations via the National Privacy Principles (NPPs), or an approved privacy code.[72] The Victorian Act regulates the practices of state government agencies by the application of IPPs, which are similar to the Commonwealth NPPs.[73]

5.38 All three sets of privacy principles deal with the following matters:

- *Collection of personal information:* collection must be necessary for the activities of those who collect the information; information must be collected lawfully and fairly; and, at the time it is collected, individuals must be told who is collecting the information and how it will be used.
- *Use and disclosure of personal information:* as a general principle, information can only be used or disclosed for its original purpose, unless the person has consented to its use or disclosure for another purpose.
- *Accuracy of personal information:* reasonable steps must be taken to ensure that personal information is accurate, complete and up-to-date.
- *Security of personal information:* reasonable steps must be taken to protect the personal information from misuse, loss, unauthorised access, modification or disclosure.
- *Openness in relation to the practices:* those who collect personal information must set out their practises in a publicly available document.
- *Access and correction rights:* as a general principle, individuals must be given access to their personal information and must be allowed to correct it or attach a statement claiming that the information is not accurate, complete or up-to-date.

In addition, the NPPs and the Victorian IPPs also deal with:

- *Unique identifiers:* Private sector organisations and Victorian government organisations are generally precluded from adopting as their own or using or disclosing unique identifiers assigned by government agencies.
- *Anonymity:* private sector organisations and Victorian government organisations must give people the option of entering into transactions anonymously where it is lawful and practicable.[74]
- *Restrictions on transborder data flows:* as a general principle, private sector organisations and Victorian government organisations can transfer personal information about an individual to a foreign jurisdiction only if they believe that the information will be protected by a law or a contract which contains principles similar to the information privacy principles or if the individual gives consent.[75]
- *Special provisions for sensitive personal information:* a higher level of protection applies to sensitive personal information, such as information about a person's health, political or religious beliefs or affiliation, and sexual preference, held by private sector organisations. Subject to some exceptions, sensitive information may be collected only with the individual's consent.

Background to privacy legislation

5.39 The ALRC conducted an extensive inquiry into privacy in the early 1980s and published a report in 1983[76] which recommended the enactment of privacy legislation based on principles derived from the Organisation for Economic Co-operation and Development (OECD) guidelines that were developed during the 1970s.

5.40 The Commonwealth Privacy Act was enacted in 1988, at a time when there were widespread concerns about the proposed introduction of an Australian identity card and the creation of an enhanced tax file number regime.[77] Those concerns focussed on the privacy threats created by the capacity of computer technology to link data about identifiable individuals.

5.41 The Privacy Act (Cth) was confined originally to Commonwealth public agencies. Over time, however, it became apparent that privacy concerns were not limited to these agencies. In addition, a new requirement for EU member countries to comply with the European Union (EU) Data Protection Directive[78] increased pressure on countries outside the EU to ensure that their data protection regimes met the EU requirements. As a result, the Commonwealth government extended the operation of the Privacy Act in 2000 by adding a set of National Privacy Principles[79] to regulate some private sector organisations.[80] The focus of this new legislation was again on computer technology, with specific reference to the impact of the internet.[81]

5.42 In 2000, Victoria enacted the *Information Privacy Act* (IPA (Vic)), which establishes a regime for the responsible collection and handling of personal information in the Victorian public sector. The Act contains information privacy principles which are very similar to the private sector principles (NPPs) in the Commonwealth legislation. A key focus of the legislation is computer technology and the uptake of e-commerce,[82] with emphasis upon the potential for technological developments to impact on privacy.[83]

ALRC reform proposals

5.43 In August 2008, the ALRC reported on the extent to which the Privacy Act (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia (ALRC Privacy Report).[84] The 2700 page report includes 295 recommendations, which, if implemented, would result in a large-scale overhaul of privacy regulation in Australia.

5.44 The ALRC recommends the creation of a unified set of privacy principles that apply to all federal government agencies and the private sector.[85] The ALRC also recommends these principles apply to state and territory government agencies through an intergovernmental cooperative scheme.[86] These steps are designed to ensure that, subject to limited exceptions, the same privacy principles apply across Australia, no matter what kind of agency or organisation is handling the information.

69 *Privacy Act 1988* (Cth); *Information Privacy Act 2000* (Vic).

70 *Privacy Act 1988* (Cth) div 3.

71 *Privacy Act 1988* (Cth) ss 6 and 9. The Act also requires agencies to ensure that private sector organisations with whom they contract to provide public services do not breach the IPPs. *Privacy Act 1988* (Cth) s 95B.

72 *Privacy Act 1988* (Cth) s 13A and sch 3 [the National Privacy Principles].

73 These laws are supplemented by the *Health Records Act 2001* (Vic), which regulates the handling of health information by Victorian government agencies and by private sector bodies operating within Victoria.

74 The anonymity principle is in only the private sector National Privacy Principles (and not the Information Privacy Principles): *Privacy Act 1988* (Cth) sch 3 (NPP 8) cf s 14.

75 Restrictions on transborder data flows is not explicitly covered by the public sector Information Privacy Principles: see *Privacy Act 1988* (Cth) sch 3 (NPP 9).

76 See Australian Law Reform Commission, *Privacy*, Report No 22 (1983). The report included a draft Privacy Bill based on a set of information privacy principles and recommended the appointment of a new Privacy Commissioner.

77 The new regime required the reporting of tax file numbers in specific contexts such as claims for government benefits with a view to reducing tax evasion. See Lee Bygrave, 'The Privacy Act 1988 (Cth): A Study in the Protection of Privacy and the Protection of Political Power' (1990) 19 *Federal Law Review* 128, 138.

78 The European Parliament and the Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31

79 These were based on set of National Principles For The Fair Handling of Personal Information developed by the then Privacy Commissioner in consultation with the private sector for the purpose of a voluntary code of practice: see National Principles For The Fair Handling of Personal Information (1999) <www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_1.86.pdf> at 7 January 2009.

80 *Privacy Amendment (Private Sector) Act 2000* (Cth).

81 For example, there was specific concern about the 'development of potentially invasive techniques such as collecting and analysing "electronic footprints", and devices such as "cookies"': see *Bills Digest No. 193 1999-2000: Privacy Amendment (Private Sector) Bill 2000*, Parliament of Australia Parliamentary Library <www.aph.gov.au/library/pubs/bd/1999-2000/2000BD193.htm> at 7 January 2009.

82 'Until a culture is established which recognises and responds to privacy concerns, Victorians will not take full advantage of the considerable benefits that new information and communications technologies have to offer.': Victoria, *Parliamentary Debates,* Legislative Assembly, 26 May 2000, 1906 (John Brumby).

83 'Over the last five years technology has created the capacity to compile, manipulate and match data on a scale that was inconceivable 20 years ago.': Victoria, *Parliamentary Debates,* Legislative Assembly, 26 May 2000, 1905 (John Brumby).

84 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008).

85 Ibid 110-111.

86 Ibid 25 (Recommendation 3– 4).

Chapter 5 Current Law

5.45 The ALRC proposes that 'principles-based regulation' be the primary method of regulating information privacy in Australia, supplemented by specific rules for some industries.[87] The ALRC recommends the following three-tired approach for Commonwealth regulation of information privacy:

- high-level principles of general application
- regulations and industry codes[88] for those practices requiring greater or more specific rules
- guidance issued by the Federal Privacy Commissioner and other relevant regulators.[89]

5.46 The ALRC Privacy Report contained a number of recommendations that are relevant to surveillance in public places. These will be addressed throughout the following discussion.

Information privacy laws and public place surveillance

5.47 Information privacy laws regulate the collection and handling of personal information. These laws govern some aspects of public place surveillance,[90] in limited circumstances. First, in order for surveillance activities to be regulated by the collection limitation principles, the information in question must be recorded. Section 3 of the IPA (Vic) defines 'personal information' as 'information or an opinion…that is recorded in any form'. Section 16B of the Privacy Act provides that in order for the Act to apply in relation to the collection of personal information, information must be collected for inclusion in a record.

5.48 Second, information must be collected about an individual who is identifiable, or potentially identifiable.[91] While photographs and CCTV footage may constitute personal information because they contain information about individuals, such as what they are doing and with whom, they would normally be identifiable only to persons who know the individual in the photograph or footage.[92] The extent to which photographs and footage produced by generalised surveillance activities meet the law's requirement of 'identifiability' remains uncertain.[93] In *Re Pasla and Australian Postal Corporation*,[94] a film was deemed to fall within the Privacy Act (Cth) but without reasons given.[95] In *Re Smith v Police (Vic)*,[96] a 'mugshot' of a convicted person was deemed to fall within the IPA (Vic).[97] It appears that if identity can be ascertained by reference to extrinsic material without amounting to an obscure or lengthy process, it falls within the ambit of the Acts.[98] Nevertheless, the ALRC has recently recommended that the Federal Privacy Commissioner clarify this issue.[99]

5.49 Third, information privacy laws do not apply to all members of the community. They apply to government agencies and larger businesses only—individuals and small businesses are not covered. Specifically, the IPA (Vic) applies to Victorian government agencies[100] and some Victorian government contractors.[101] The Privacy Act (Cth) applies to Commonwealth government agencies[102] and businesses with a gross annual turnover of over $3 million.[103]

5.50 The commission notes the Commonwealth and Victorian Privacy Commissioners have provided little guidance about what CCTV operators and users of other surveillance devices capable of capturing personal information must do to comply with relevant privacy laws.[104] In contrast, privacy commissioners in some other countries have developed specific codes of practice or guidelines to clarify that information privacy laws do apply, for example, to video surveillance.[105]

5.51 As we suggested earlier, a number of privacy principles relate directly to public surveillance practices,[106] particularly those regulating collection, sensitive information, notification, openness and anonymity. These are discussed below.

Collection principle

5.52 Information privacy laws prohibit an organisation or agency from collecting personal information unless the information 'is necessary for one or more of its functions or activities'.[107] The Privacy Commissioner was required to apply this principle to information collected through surveillance in her handling of a complaint raised in 2006. The complainant's wife was the subject of surveillance by the respondent, a contracted service provider to a statutory authority, in relation to her claim for compensation due to injury. The complainant alleged that in collecting information about his wife, the respondent had also collected information about him that was not necessary for the respondent's functions.

5.53 The Privacy Commissioner noted that 'when an individual is surveilled lawfully and appropriately in the circumstances, information collected will inevitably include a certain amount of information about other people who interact closely with the subject of the surveillance'. The test, according to the Commissioner, is whether a reasonable person would find sufficient connection between the subject of surveillance and the other party. If so, then the information collected is relevant information. In this case the Commissioner decided that there was a sufficient connection between the complainant and his wife, and that the collection was necessary to the respondent's functions.[108]

5.54 Organisations and agencies 'must collect personal information only by lawful and fair means and not in an unreasonably intrusive way'.[109] Significantly for users of surveillance, the Federal Privacy Commissioner has interpreted 'fair' collection to mean 'without intimidation or deception',[110] and not through covert means (subject to exceptions, for example law enforcement purposes).

5.55 Agencies and organisations which have collected personal information about an individual are required to take reasonable steps to ensure that the person is aware of a number of matters in relation to that information. These include the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; the organisations to whom the organisation usually discloses information of that kind; any law that requires the particular information to be collected; and the consequences for the individual if the information is not provided.[111]

5.56 The obligation to notify an individual that his or her personal information has been collected applies in circumstances where the individual may not be aware of the collection. This obligation may apply where personal information is collected by surveillance technology, for example CCTV

87 Ibid 111.

88 While both codes and regulations are mandatory, the ALRC distinguishes codes from regulations by the fact that codes merely 'prescribe how a principles is to be applied or complied with' and 'cannot derogate from the principles in the way that subordinate legislation, such as regulations, can': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [4.51]–[4.52].

89 That is, advice, not legally binding, on how to comply with privacy principles, as most users will only be subject to privacy principles, rather than regulations and codes. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008)111.

90 See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1 – 3* (1994) 11-12; Office of the Victorian Privacy Commissioner, *Short Guide to the Information Privacy Principles* (2006) 13; Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info Sheet 05.03 (2003) 3.

91 Information privacy laws regulate the collection and handling of 'personal information' only. The definition of personal information requires that the information must be able to identify, or potentially identify a person: *Privacy Act 1988* (Cth) s 6; *Information Privacy Act 2000* (Vic) s 3.

92 Christa Ludlow, '"The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135, 145.

93 Ibid.

94 (1990) 20 ALD 407.

95 Christa Ludlow, '"The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135, 145.

96 [2005] VCAT 654.

97 Christa Ludlow, '"The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135, 145.

98 Ibid 145-146 discussing *Police Force of Western Australia v Ayton* [1999] WASCA 233.

99 See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) 312–16 (Recommendation 6–3).

100 *Information Privacy Act 2000* (Vic) s 9.

101 Those whose contracts specifically require them to comply with the Act. See *Information Privacy Act 2000* (Vic) s 17(2).

102 *Privacy Act 1988* (Cth) s 6(1) (definition of 'agency') and s 7. Schedule 2 of the *Freedom of Information Act 1982* (Cth) contains exclusions in respect of ASIO, ASIS, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation and the Defence Signals Directorate.

103 *Privacy Act 1988* (Cth) s 6D(1)–(2). Note the *Privacy Act 1988* (Cth) ss 6D(4) excludes some small business from this exemption, including businesses that are contractors to Commonwealth government agencies, and businesses that trade in personal information (the latter would thus include private investigators). The commission notes that the ALRC has recommended the small business exemption be removed from privacy laws: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) 53 (Recommendation 39–1). This would bring Australian privacy laws further into line with privacy regimes in other jurisdictions, including the European Union, which has cited the small business exemption as an obstacle to Australia's privacy laws being deemed 'adequate'. See Article 29 Data Protection Working Party, European Commission, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance,* adopted on 11 February 2004, 6; and Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 2: Final Report 108* (2008) [39.45]–[39.50].

104 The exception is the Victorian Privacy Commissioner's Fact Sheet on Mobile Phones as a Surveillance Device: Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003).

105 See, eg, Office of the Privacy Commissioner of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (March 2006) <www.privcom.gc.ca/information/guide/vs_060301_e.asp> at 13 January 2009; European Commission for Democracy for Law (Venice Commission), Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights study no 404 (2007); and European Commission for Democracy for Law (Venice Commission), Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection: Adopted by the Venice Commission at its 71st Plenary Session (Venice, 1–2 June 2007) CDL-AD(2007)027 (2007).

106 As discussed in Chapter 1, we have focussed on surveillance *practices.* The commission notes the ALRC has made a number of recommendations regarding principles relating to the *use* and *disclosure* of information that would, if enacted, strengthen current privacy protections and reduce ambiguity in relation to the application of the principles. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) 25–90.

107 *Privacy Act 1988* (Cth) sch 3 (NPP 1.1); *Information Privacy Act 2000* (Vic) sch 1 (IPP 1.1).

108 *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6.

109 *Privacy Act 1988* (Cth) sch 3 (NPP 1.2); *Information Privacy Act 2000* (Vic) sch 1 (IPP 1.2).

110 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001) 27.

111 *Privacy Act 1988* (Cth) sch 3 (NPP 1.3); *Information Privacy Act 2000* (Vic) sch 1 (IPP 1.3).

systems and radio frequency identification (RFID) tags. The commission notes the ALRC has suggested this obligation should not be imposed where an individual is aware of the collection,[112] for example, surveillance systems operating on cashless toll roads. The ALRC has recommended the Federal Privacy Commissioner provide guidance to this effect.[113]

5.57 The ALRC recommends the Federal Privacy Commissioner develop guidelines to assist agencies and organisations to comply with notification requirements—in particular, addressing the circumstances when it would and would not be reasonable for an agency or organisation to take no steps to notify individuals.[114]

Sensitive information principle

5.58 Information privacy laws separately regulate the collection of a subclass of personal information known as 'sensitive information'.[115] Information relating to a range of matters such as race or ethnic origin, political or religious beliefs, trade union membership and sexual orientation falls within this category.[116] As this information is highly personal and may provide the basis for discrimination, information privacy laws place extra restrictions on its collection, use and disclosure.

5.59 Organisations and agencies are prohibited from *collecting* sensitive information about an individual except in limited circumstances, including where the individual has given his or her consent to its collection.[117] Information privacy laws do not define consent other than to provide that it may be express or implied.[118]

5.60 If a CCTV camera, or other surveillance device, captures and records an image that identifies an individual and also identifies one of their personal characteristics, this information may be classed as 'sensitive'. In most cases where sensitive information is collected through surveillance, express consent from an individual will not be provided, and organisations and agencies will be required to demonstrate that they have obtained implied consent.[119] The Federal Privacy Commissioner notes that implied consent arises 'where consent may reasonably be inferred in the circumstances from the conduct of the individual.'[120]

5.61 The Federal Privacy Commissioner has published *Guidelines to the National Privacy Principles* which deal with the collection of sensitive data through surveillance.[121] The Guidelines state that where an agency or organisation has fulfilled 'notification' requirements under privacy legislation, the agency or organisation will have a 'strong basis' for assuming it has the individual's consent to use or disclose their information.[122] The notification requirements are fulfilled where the agency or organisation has taken 'reasonable steps' to ensure the person is aware of a number of matters in relation to the collection of their sensitive information.[123]

5.62 The requirement for an individual's consent to be obtained before an agency or organisation can collect their sensitive information raises a number of issues for users of surveillance. While an agency or organisation may strategically place notices containing appropriate information, the amount of information required may make it difficult for some people to read it comprehensively. Additionally, consideration must be made for people unable to read the notice, for example minors, non-English readers and sight-impaired people.[124]

5.63 The ALRC explored this area in their recent Privacy Report, noting:

> *There is a pressing need for contextual guidance on consent. What is required to demonstrate that consent has been obtained is often highly dependant on the context in which personal information is collected, used and disclosed.*[125]

5.64 The ALRC has recommended that the Federal Privacy Commissioner provide further guidance on the meaning of consent, including the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained.[126]

Anonymity principle

5.65 Information privacy laws require that wherever lawful and practicable, people must have the option of not identifying themselves when entering transactions with an organisation.[127] This principle is of increasing relevance because surveillance technologies have greater capacity to identify people as they become more sophisticated. An example is the payment systems used on Victorian toll roads which effectively remove any opportunity for anonymous travel as they identify vehicles (and their registered owners). The Cyberspace Law and Policy Centre notes:

> *Had sufficient attention been paid to an anonymity/pseudonymity principle at the outset, it should have been possible to design automated toll roads that either respected the right of anonymous travel (through the use of pre-paid debit tags) or at least offered 'pseudonymous' accounts where identification of the actual user would only be triggered by exceptional events, (such as non-payment, accidents or crime).*[128]

Openness principle

5.66 The openness principle is designed to ensure that personal information-handling practices of agencies and organisations are transparent.[129] Under Commonwealth and Victorian legislation, organisations and agencies must produce clearly expressed policies about their management of personal information in a publicly available document.[130] On request they must also take reasonable steps to let a person know generally what sort of personal information they hold, for what purposes, and how they collect, hold, use and disclose that information.[131] Surveillance users whose practices are capable of capturing personal information, and who are not exempt from information privacy laws, must comply with this principle.

Limitations

5.67 While information privacy laws apply to some forms of public place surveillance, those laws were not designed specifically to regulate the use of surveillance practices. As discussed above, the impetus for their enactment derived from concerns about public confidence in an enhanced tax file number system, in e-commerce and a desire to meet EU standards. For this and a number of other reasons, information privacy laws are limited in their application to public place surveillance.

5.68 Information privacy laws are concerned with the collection, storage and use of 'personal information' only. The extent to which surveillance practices can capture personal information is unclear and may remain so because of uncertainty about the extent to which material collected by the use of some common surveillance devices is 'personal information'.

5.69 Further, as discussed above, information privacy laws do not apply to all members of the community—private individuals[132] and businesses with an annual turnover of less than $3 million do not have to comply with the obligations imposed by either the Privacy Act (Cth) [133] or the IPA (Vic).

5.70 Finally, there appears to be a general lack of awareness about the applicability of the laws. Many people we consulted seemed unaware that information privacy laws may apply to some forms of surveillance. For example, some businesses discussed their policies on releasing CCTV footage to third parties without reference to the relevant principles in the Privacy Act.[134]

Binding codes of practice

5.71 Currently, both the Federal Privacy Commissioner and the Victorian Privacy Commissioner have the power to approve a code of practice which may operate as an alternative to the relevant privacy principles.[135] An organisation may submit a code of practice to a Privacy Commissioner for approval.[136] In order to approve a code, a Privacy Commissioner must be satisfied that, among other things, the code is at least as stringent as the applicable privacy principles.[137] A breach of an approved code will have the same effect as a breach of the relevant privacy principle.[138]

112 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) 787.

113 Ibid 38 and 803 (Recommendation 23–3(a)(iv)).

114 Ibid 38 and 803 (Recommendation 23–3).

115 *Privacy Act 1988* (Cth) sch 3 (NPP 10); *Information Privacy Act 2000* (Vic) sch 1 (IPP 10).

116 *Privacy Act 1988* (Cth) s 6(1); *Information Privacy Act 2000* (Vic) sch 1.

117 *Privacy Act 1988* (Cth) sch 3 (NPP 10.1(a)); *Information Privacy Act 2000* (Vic) sch 1 (IPP 10.1(a)).

118 *Information Privacy Act 2000* (Vic) s 3.

119 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001) 18.

120 Ibid 22.

121 Ibid.

122 Ibid 33.

123 Including the organisation's identity and contact details; the fact that he or she can access the information; the purposes of collection; and the organisations to whom the organisation usually discloses information of that kind; any law that requires the particular information to be collection; and the consequences for the individual if the information is not provided. See *Privacy Act 1988* (Cth) sch 3 (NPP 1.3); *Information Privacy Act 2000* (Vic) sch 1 (IPP 1.3).

124 This problem has also been noted in Article 29 Data Protection Working Party, European Commission, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance* Adopted on 11 February 2004:11750/02/EN: WP89 (2004) 22.

125 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) 683.

126 Ibid 686 (Recommendation 19–1).

127 *Privacy Act 1988* (Cth) sch 3 (NPP 8); *Information Privacy Act 2000* (Vic) sch 1 (IPP 8).

128 Graham Greenleaf, Nigel Waters, and Lee Bygrave, 'Strengthening Uniform Privacy Principles: An Analysis of the ALRC's Proposed Principles: Submission to the Australian Law Reform Commission on the Review of Australian Privacy Laws, Discussion Paper 72' (2007) 14.

129 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) [24.1].

130 *Privacy Act 1988* (Cth) sch 3 (NPP 5.1); *Information Privacy Act 2000* (Vic) sch 1 (IPP 5.1).

131 *Privacy Act 1988* (Cth) sch 3 (NPP 5.2); *Information Privacy Act* 2000 (Vic) sch 1 (IPP 5.2).

132 *Privacy Act 1988* (Cth) s 16E.

133 The *Privacy Act 1988* (Cth) s 6D exempts a 'small business' from the definition of an 'organisation', and therefore from the operation of the Act.

134 Roundtable 14.

135 For any specified information, organisation, activity or profession (or class thereof): *Privacy Act 1988* (Cth) s 18BB(7); *Information Privacy Act 2000* (Vic) s 18(3).

136 *Privacy Act 1988* (Cth) s 18BA; *Information Privacy Act 2000* (Vic) s 19.

137 *Privacy Act 1988* (Cth) s 18BB(2)(a); *Information Privacy Act 2000* (Vic) s 18(2)(a).

138 *Privacy Act 1988 (Cth) s 16A; Information Privacy Act 2000* (Vic) s 21.

Chapter 5 Current Law

5.72 There have been no codes approved under the IPA (Vic). There are currently two codes operating in Victoria under the Privacy Act (Cth), the *Biometrics Institute Privacy Code* and the *Market and Social Research Privacy Code*.[139] The principles in these codes are substantially the same as the NPPs. Where the principles in the *Biometrics Institute Privacy Code* differ, they 'intend to provide additional privacy protection to end-users,'[140] including, for example, the requirement that, wherever practicable, biometric information must be encrypted after collection.[141] The principles in the *Market and Social Research Privacy Code* 'seek to give effect to the Privacy Act (Cth) in a manner that is tailored to the research context, while providing the public and business community with the assurances needed to encourage informed and willing participation in market and social research activities.'[142] Administration of the codes is the responsibility of the relevant industry bodies[143] and is subject to review by an independent panel and the Privacy Commissioner.

5.73 The Privacy Act (Cth) also allows for the creation of codes for media organisations' acts or practices conducted 'in the course of journalism'.[144] Unlike the codes described above, there is no requirement that the codes offer equivalent protection as the NPPs. Instead, media organisations are merely required to observe published standards that 'deal with privacy in the context of the activities of a media organisation'.[145]

5.74 Media codes typically deal with surveillance in the following ways:

- referring to laws that impose limits on media surveillance
- pointing out that private activities can on occasion take place in public places
- requiring a public interest justification for breaches of the right to privacy with respect to private matters
- discouraging covert surveillance unless justified by public interest.[146]

5.75 In its Privacy Report the ALRC found variability among the established codes.[147] It also found that some media codes lacked specific privacy provisions, and that only two codes dealt with children's privacy.[148]

Enforcement

5.76 The Federal and Victorian Privacy Commissioners have the power to receive complaints relating to agencies and organisations that may have contravened information privacy laws in their jurisdiction.[149]

5.77 The Federal Privacy Commissioner received 1126 new complaints in 2007–08.[150] The most frequently raised concerns were (in ascending order) about use or disclosure,[151] security[152] and collection.[153] Complaints were most frequently about private organisations.[154] The Victorian Privacy Commissioner received 51 new complaints in 2007–08.[155] The most common complaints were about state government departments[156] followed by statutory authorities[157] and contracted service providers.[158] Data security was the subject of the largest number of complaints,[159] closely followed by use and disclosure of information.[160]

5.78 The Federal Privacy Commissioner is empowered to conduct an investigation into a complaint,[161] including the power to obtain information and documents[162] and to examine witnesses.[163] After investigating the complaint, the Commissioner may make a determination dismissing the complaint,[164] or, if the complaint is upheld, make a declaration, as well as a non-binding order for the payment of damages,[165] or one which requires the respondent to take any reasonable action to redress any loss or damage suffered by the complainant.[166] The Commissioner may institute proceedings in the Federal Court or Federal Magistrates Court to enforce a determination.[167]

5.79 The Victorian Privacy Commissioner has the power to obtain information and documents, or require a person to answer questions, in relation to the conciliation of a complaint.[168] Under the IPA (Vic), conciliation of a complaint may involve an undertaking by one of the parties to take some action, including the provision of compensation for humiliation and distress, or an apology.[169]

5.80 The Victorian Privacy Commissioner may serve a compliance notice on an organisation if it appears the organisation has acted in a way that 'constitutes a serious or flagrant contravention' of an IPP or applicable code of practice.[170] The organisation must have committed the breach at least five times within the previous two years for a notice to be served.[171] It is an offence not to comply with a compliance notice.[172] The Victorian Privacy Commissioner may require the provision of information or documents[173] and examine witnesses when exercising this power.[174] The Commissioner has issued two compliance notices.[175]

5.81 At the request of the complainant, the Victorian Privacy Commissioner may refer a complaint to the Victorian Civil and Administrative Tribunal (VCAT) for adjudication if conciliation fails.[176] The Minister may refer a complaint directly to VCAT if he or she considers that the complaint 'raises an issue of important public policy'.[177] If VCAT finds a complaint proven, it may make various orders including a direction that the respondent not continue, or repeat, any action and an order for the payment of compensatory damages not exceeding $100,000.[178]

OTHER AUSTRALIAN JURISDICTIONS

5.82 In its review of Australian privacy law, the ALRC recently noted that each Australian state and territory regulates the management of personal information by public authorities through either a legislative regime or an administrative scheme, and proceeded to describe them.[179]

5.83 NSW was the first state to enact public sector privacy laws.[180] *The Privacy and Personal Information Protection Act 1998* (NSW) contains IPPs that regulate the way NSW public sector agencies handle personal information—these are modelled on the federal IPPs which cover the federal public sector.

5.84 The ACT public sector is regulated by legislation[181]which is based on the Commonwealth Privacy Act. The Federal Privacy Commissioner administers the Act on behalf of the ACT government. The Northern Territory has combined its information privacy, freedom of information and public records laws into a single Act, the *Information Act 2002* (NT). The Act contains 10 IPPs[182] based on the federal NPPs.[183]

5.85 The Queensland and South Australian public sectors are regulated by administrative schemes which contain IPPs based on the federal IPPs.[184] In Western Australia, some privacy principles are included in the *Freedom of Information Act 1992* (WA).[185] The Information Privacy Bill 2007 (WA) was introduced into the Western Australian Parliament in March 2007.[186] The Bill proposes to regulate the handling

138 *Privacy Act 1988 (Cth) s 16A; Information Privacy Act 2000* (Vic) s 21.

139 Office of the Privacy Commissioner, *Register of Approved Privacy Codes* (2009) available at <www.privacy.gov.au/business/codes/index.html#1> at 29 January 2009. Applications for the *Australian Casino Association Privacy Code* and *Internet Industry Privacy Code* are also currently being considered: Office of the Privacy Commissioner, *Code Applications Currently Being Considered* (2009) available at <www.privacy.gov.au/business/codes/index.html#1> at 29 January 2009.

140 Biometrics Institute, *Biometrics Institute Privacy Code* (2006) 1.

141 Ibid 16-18.

142 Association of Market and Social Research Organisations, *Market and Social Research Privacy Code* (2007) 1.

143 The Association of Market and Social Research Organisations and the Biometrics Institute.

144 *Privacy Act 1988* (Cth) s 7B(4)(a).

145 *Privacy Act 1988* (Cth) s 7B(4)(b).

146 See, eg, Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005); and *Privacy Standards,* Australian Press Council <www.presscouncil.org.au/pcsite/complaints/priv_stand.html> at 7 July 2008.

147 Australian Law Reform Commission, *Review of Australian Privacy Law: Volume 2: Discussion Paper* Discussion Paper 72 (2007) 1083 [38.9].

148 Ibid 1083–4 [38.9].

149 *Privacy Act 1988* (Cth) s 36(1); *Information Privacy Act 2000* (Vic) s 25(1).

150 Office of the Federal Privacy Commissioner, *Annual Report 2007/2008* (2008) 43.

151 41% of IPP allegations. Office of the Federal Privacy Commissioner, *Annual Report 2007/2008* (2008) 45.

152 17% of IPP allegations. Ibid.

153 15% of IPP allegations. Ibid.

154 This has been the case since the Commissioners' role was extended to the private sector. Office of the Federal Privacy Commissioner, *Annual Report 2007/2008* (2008) 43.

155 This is a slight decrease from the 54 complaints that were received in the previous year: Office of the Victorian Privacy Commissioner, *Annual Report 2007-08* (2008) 20.

156 Over 40% (21 complaints): Ibid.

157 Nine complaints: Ibid.

158 Seven complaints: Office of the Victorian Privacy Commissioner, *Annual Report 2007-08* (2008) 20.

159 31 complaints: Ibid.

160 29 complaints: Ibid.

161 *Privacy Act 1988* (Cth) s 40.

162 *Privacy Act 1988* (Cth) s 44.

163 *Privacy Act 1988* (Cth) s 45.

164 *Privacy Act 1988* (Cth) s 52(1)(a).

165 *Privacy Act 1988* (Cth) s 52(1)(B)(iii).

166 *Privacy Act 1988* (Cth) s 52(1)(B)(ii).

167 *Privacy Act 1988* (Cth) s 55A.

168 *Information Privacy Act 2000* (Vic) s 34. The Commissioner also has the power to decline, dismiss, refer or conciliate the complaint in certain circumstances: *Information Privacy Act 2000* (Vic) ss 29, 30, 33, 34A.

169 For example, see *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6, where the respondent agreed to pay the complainant compensation for humiliation and distress; to formally apologise; and to destroy all surveillance-collected information it held regarding the complainant.

170 *Information Privacy Act 2000* (Vic) s 44(1)(a).

171 *Information Privacy Act 2000* (Vic) s 44(1)(b).

172 In the case of a body corporate, the offence attracts 3000 penalty units; in any case 600 penalty units. *Information Privacy Act 2000* (Vic) s 48.

173 *Information Privacy Act 2000* (Vic) s 45.

174 *Information Privacy Act 2000* (Vic) s 46.

175 Office of the Victorian Privacy Commissioner, Report 03.06 *Mr C's Case* (2006) 47; Office of the Victorian Privacy Commissioner, Report 01.06 *Jenny's Case* (2006) 79.

176 However, if the Commissioner doesn't consider conciliation appropriate, or if conciliation fails, the complainant has the power to request the commissioner refer the complaint to VCAT: *Information Privacy Act 2000* (Vic) ss 32 and 37.

177 *Information Privacy Act 2000* (Vic) s 31(1).

178 *Information Privacy Act 2000* (Vic) ss 43(1) and (2).

179 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) [2.10].

180 Ibid [2.14].

181 *Australian Capital Territory Government Service (Consequential Provision) Act 1994* (Cth).

182 *Information Act 2002* (NT) sch.

183 Northern Territory, *Parliamentary Debates,* Legislative Assembly, 14 August 2002 (Peter Toyne, Minister for Justice and Attorney-General) <http://notes.nt.gov.au/lant/hansard/hansard9.nsf/WebbyMember/CF95BD87835772B869256C33001A1C79?opendocument> at 13 January 2009.

184 In Queensland, details of the scheme are provided in *Information Standard 42—Information Privacy* (IS 42), issued by the Queensland Department of Innovation and Information Economy under the *Financial Management Standard 1997* (Qld): See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) [2.36]-[2.37]; and *Queensland Government Information Privacy Principles (IPPs)*, Queensland Government (21 February 2006) <www.privacy.qld.gov.au/principles.htm#3> at 21 January 2009. In South Australia, the scheme is in the form of an administrative instruction - *PC012—Information Privacy Principles Instruction* (1992) - issued by the South Australian Department of Premier and Cabinet: see *PC012 – Information Privacy Principles Instruction,* Government of South Australia (1992) <www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf> at 21 January 2009. See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) [2.58].

185 For example, the Act provides for access to documents and the amendment of personal information in a document held by an agency that is inaccurate, incomplete, out of date or misleading: *Freedom of Information Act 1992* (WA) s 45(1).

186 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 March 2007, 824–7 (Jim McGinty, Attorney-General).

of personal information in the state public sector[187] through a set of IPPs, which draw heavily on the federal NPPs, and the Victorian IPPs.[188] The Bill has not yet passed through both houses of the Western Australian Parliament.[189]

OTHER LEGISLATION

VICTORIA

5.86 Some of the most offensive forms of surveillance and behaviours incidental to surveillance are separate criminal offences. For example, the *Crimes Act 1958* (Vic) makes it an offence punishable by up to 10 years imprisonment to stalk another person with the intention of causing them physical or mental harm, or to fear for their safety.[190] Behaviour which can amount to stalking includes not only following a person, but also tracing their use of the internet, email or other electronic communications, loitering outside a building, and generally keeping a person under surveillance.[191]

5.87 Various uses of surveillance material that involve children and sexual acts may contravene child pornography offences. For example, the *Crimes Act 1958* (Vic) makes it an offence punishable by imprisonment of up to 10 years to make or produce child pornography. A photograph taken of an underage person in a change room might constitute such an act. It is also an offence under the Commonwealth Criminal Code to use a telecommunications carrier (whether by use of a telephone or the internet) to access or transmit child pornography material.[192] Similarly, it is an offence under the Code to use a telecommunications carrier in a way that would be menacing, harassing or offensive.[193] The offence covers a situation where someone photographs another 'getting undressed when they are unaware, and sends that picture to another phone or to an internet site'.[194]

5.88 Section 17 of the *Summary Offences Act 1966* (Vic) makes it an offence to engage in behaviour that is 'indecent, offensive or insulting' in or near a public place. The law was used to prosecute upskirting, however, since September 2007, upskirting is a separate offence.[195] The new legislation followed a spate of incidents in which men were caught secretly filming up the skirts of women on public transport and at public events.[196]

5.89 There are some laws that regulate the use of surveillance by specific businesses and organisations. For example, the *Transport (Taxi-Cabs) Regulations 2005* (Vic) makes it illegal to drive a taxi cab that is not fitted with a functioning camera or to interfere with such a camera.[197] In addition, the *Transport Act 1983* (Vic) prohibits anyone from downloading, printing or disclosing any images or other data from security cameras in taxis, except with the authorisation of the Director of Public Transport.[198]

5.90 Bars[199] and casinos[200] have specific laws governing the installation and operation of security cameras. Laws governing private investigators and private security agents indirectly regulate surveillance by requiring training for surveillance users, which may include information on how to comply with existing laws on surveillance.[201]

COMMONWEALTH

5.91 There are a number of Commonwealth laws which authorise the use of surveillance for law enforcement purposes and for the protection of national security.

5.92 While surveillance of telecommunications systems[202] is generally prohibited[203] by the TIA, there are detailed exceptions for national security and law enforcement activities.[204] Warrants may be issued by a court or tribunal for law enforcement activities, and by the Commonwealth Attorney-General for national security activities.[205]

5.93 The TIA has a number of important limitations. First, the Act does not regulate some forms of communication surveillance. Because the TIA is confined to communications 'passing over' the telecommunications system, the Act does not prohibit recording a telephone conversation with a device placed close to a telephone handset.[206] Another important limitation is that the TIA is limited to the telecommunications networks. The Act does not cover a communication that takes place via radio waves (such as occurs between two 'walkie talkies' or Bluetooth-enabled[207] devices) or infrared light waves.[208]

5.94 The *Australian Security Intelligence Organisation Act 1979* (Cth) authorises Australian Security Intelligence Organisation (ASIO) officers to use data surveillance,[209] listening[210] and tracking *devices,*[211] *if they have received a warrant from the relevant Minister. T*he Defence Imagery and Geospatial Organisation,[212] the Defence Signals Directorate,[213] and the Australian Secret Intelligence Service[214] are also granted broad investigative powers under the Act. The *Aviation Transport Security Act 2004* (Cth) allows for the use of optical surveillance devices at airports and on board aircraft without a warrant.

5.95 The *Crimes Act 1914* (Cth) permits the Australian Federal Police and State and Territory police to gather information in relation to terrorist acts, without the need for a warrant in 'Commonwealth places'[215] and prescribed security zones.[216] The Act also empowers the Australian Federal Police and State and Territory police to obtain information or documents about terrorist acts from operators of aircraft or ships without a warrant.[217]

COMMON LAW PROTECTIONS

5.96 As well as the laws made by Commonwealth, State and Territory parliaments, Australia has a system of common law that is developed though decisions of the courts. In some instances, the common law allows people to sue others when various wrongs are committed (known as 'a cause of action'). Redress is available via 'torts' (which are civil as opposed to criminal wrongs) and equitable actions, (such a 'breach of confidence'), which are derived from notions of fair and responsible behaviour. A person who has a cause of action is usually entitled to sue for compensation and other remedies, such as a declaration by a court that a person has engaged in unlawful behaviour.

5.97 The common law regulates some surveillance activities, but does so indirectly when protecting other interests, such as those in property. The interest most directly and immediately affected by surveillance activities—privacy—has not received much attention from the common law. Professor Danuta Mendelson has written:

> *Our right to privacy is relatively modern, and has received scant protection at common law. However, as society ascribes to it more value, it is possible either that a new tort protecting privacy will be recognised or that existing torts will be expanded to encompass aspects of the right to privacy.* [218]

5.98 Development of an Australian body of common law to protect the growing interest in privacy may have been hindered by the fact that 'there is no easy, embracing formula for dealing with all the

187 Information Privacy Bill 2007 [WA] cl 3(a). The Bill also proposes to regulate the handling of health information by the public and private sectors in Western Australia: cl 3(b). See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008) [2.52].

188 Western Australia, *Parliamentary Debates*, Legislative Assembly, 28 March 2007, 824–7 (Jim McGinty, Attorney-General).

189 Information Privacy Bill 2007 (WA) <www.parliament.wa.gov.au/web/newwebparl.nsf/iframewebpages/Bills+-+All> at 21 January 2009.

190 *Crimes Act 1958* (Vic) s 21A.

191 The offence does not, however, apply to the conduct associated with the conduct of official duties (for example in relation to law enforcement): *Crimes Act 1958* (Vic) s 21A(4). For examples of the approach taken by the courts in interpreting these provisions, see *R v Orgill* [2007] VSCA 236 (in relation to stalking of a child); *DPP v Sutcliffe* [2001] VSC 43 (in relation to stalking involving mail and internet correspondence); *R v Hoang* (2007) 19 VR 369 (in relation to stalking involving phone calls and letter writing).

192 *Criminal Code Act 1995* (Cth) sch [474.19].

193 *Criminal Code Act 1995* (Cth) sch [474.17].

194 'Coonan Urges Mobile Industry to Bank Reforms', *The Age* (Melbourne) <www.theage.com.au/articles/2004/09/22/1095651358042.html?from=storyrhs> at 13 January 2009.

195 *Summary Offences Act 1966* (Vic) div 4A. Penalties include three months imprisonment for observing a person's genital or anal areas from beneath and two years imprisonment for visually capturing or distributing images of a person's genital or anal region: *Summary Offences Act 1966* (Vic) ss 41A, 41B and 41C.

196 See, eg, Chris Tinkler, 'Upskirt Picture Ban', *Herald Sun* (Melbourne), 27 May 2007, 18; Steve Butcher, 'Student jailed for 'upskirting' at tennis', *The Age* (Melbourne), 6 June 2007, 12; Mark Dunn and Jacqueline Freegard, 'Perverts' snapshots hit the net', *Herald Sun* (Melbourne), 24 January 2007, 21; Georgie Pilcher, 'Sneaker Peeker Bootcam Videos up Skirts', *Herald Sun* (Melbourne), 18 January 2007, 13.

197 See *Transport (Taxi-Cabs) Regulations 2005* (Vic) regs 15 and 22. These were mentioned to the commission during Roundtable 10. Note that new Taxi Security Camera Standards will establish a minimum benchmark for camera specification and performance. See: Department of Infrastructure, *Action: The Victorian Taxi Safety Strategy: New Security Cameras for Victoria's Taxis* <www.doi.vic.gov.au/DOI/DOIElect.nsf/$UNIDS+for+Web+Display/40A969C6A7B911E4CA257332001B103B/$FILE/VTD%20Fact%20Sheet%20-%20New%20Security%20Cameras%20for%20Victoria's%20Taxis.pdf> at 14 May 2008.

198 *Transport Act 1983* (Vic) ss 158B–C.

199 *Liquor Control Reform Act 1998* (Vic) s 18B.

200 Roundtable 13. See *Casino Control Act 1991* (Vic) ss 59(2)(b), 122(r) – the Act gives the Victorian Commission for Gambling Regulation control over the operation of security cameras at gaming clubs in Victoria and requires that they develop procedures for their use.

201 For example, the *Private Agents Act 1966* (Vic) s 6 requires private agents to be licensed and the *Private Security Act 2004* (Vic) ss 25(3), 182 impose a competency requirement on both private agents and private security that includes completing approved training. One approved training program includes the law relevant to surveillance, including the storage and protection of information gathered. See Australian School of Security and Investigations, *Certificate III in Investigative Services* (2007).

202 The electronic pathways of telecommunications are public 'places' because they are accessible by members of the public.

203 *Telecommunications (Interception and Access) Act 1979* (Cth) s 7. Note also the *Criminal Code Act 1995* (Cth) outlaws a number of activities incidental to surveillance, such as being in possession of a telecommunications interception device: *Criminal Code Act 1995* (Cth) Sch 1 [474.4-474.12], [474.17], [477.1-477.3], [478.1].

204 These provisions are supplemented by state and territory legislation which requires the recording of information relating to warrants: see *Telecommunications (Interception and Access) Act 1987* (NSW); *Telecommunications (Interception) Act Northern Territory Act 2001* (NT); *Telecommunications Interception Act 1998* (SA); *Telecommunications (Interception) (State Provisions) Act 1988* (Vic); *Telecommunications (Interception) Western Australia Act 1996* (WA); *Telecommunications (Interception) Act 1999* (Tas).

205 There is also provision for the Director-General of Security to issue emergency interception warrants in specified circumstances involving a threat to security within the meaning of section 4 of the *Australian Security and Intelligence Organisation Act 1979* (Cth): see *Telecommunications (Interception and Access Act 1979* (Cth) ss 10. In addition, a member of a police force may request the interception of telecommunications where a threat to life or risk of serious injury exists: see *Telecommunications (Interception and Access) Act 1979* (Cth) s 30.

206 Prior to the inclusion of s 5D the position was less clear. In *R v Curran* (1982) 50 ALR 745, 767–768 the court held that the Act applied to this situation. However, the majority of cases expressed a contrary view: see, eg, *R v Oliver* (1984) 57 ALR 543, 548; *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580, 583. This is subject to an exception for the Australian Federal Police: *Telecommunications (Interception and Access) Act 1979* (Cth) s 5D(1)(f).

207 BlueTooth involves the use of low-power radio communications to wirelessly link phones, computers and other network devices over short distances.

208 See *Telecommunications (Interception and Access) Act 1979* (Cth) s 5 ("telecommunications system" and "telecommunications network").

209 *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A.

210 *Australian Security Intelligence Organisation Act 1979* (Cth) s 26(1)(c).

211 *Australian Security Intelligence Organisation Act 1979* (Cth) s 26A(2)(b).

212 *Intelligence Services Act 2001* (Cth) s 6B.

213 *Intelligence Services Act 2001* (Cth) s 7.

214 *Intelligence Services Act 2001* (Cth) s 6.

215 'Commonwealth place' is defined in the *Commonwealth Places (Applications of Laws) Act 1970* (Cth) s 3 as meaning 'a place… with respect to which the Parliament, by virtue of section 52 of the Constitution, has, subject to the Constitution, exclusive power to make laws for the peace, order, and good government of the Commonwealth.' For example federal national parks and airports.

216 The Minister has power to declare an area to be a prescribed security zone if he or she considers that this would prevent a terrorist act occurring or in responding to a terrorist act that has occurred: see *Crimes Act 1914* (Cth) s 3UJ.

217 *Crimes Act 1914* (Cth) s 3ZQM.

218 Danuta Mendelson, *The New Law of Torts* (2007) 6.

different practices involved' and because the proper balance to be struck between the various interests 'varies greatly and demands individualised solutions'.[219] The limited range of remedies at common law for damage, other than personal injury, may have also contributed to the fact that there have been few 'privacy' cases to assist in the formulation of broad principles.[220]

5.99 The torts of trespass and nuisance have a limited role in regulating the use of surveillance in public places, as does the action for breach of confidence. While a tort of invasion of privacy has been recognised by some Australian trial courts[221] and by appeal courts in other countries with similar legal systems,[222] there are no decisions of the High Court, or the intermediate appellate courts in Australia, which have confirmed the existence of this tort. It is possible, however, that the courts will develop a tort of invasion of privacy over time, especially if there is no further legislative action in this field.

TRESPASS, NUISANCE AND BREACH OF CONFIDENCE

5.100 In some instances, a person may take action for trespass and/or nuisance to protect their privacy[223] if surveillance activities interfere with their interest in land.[224] For example, a person may bring an action in trespass to prevent other people from entering his or her land to engage in surveillance activities. In *Lincoln Hunt (Aust) Pty Ltd v Willesee* the court held that entry onto premises by journalists with cameras rolling constituted a trespass where there had been no express or implied permission for them to enter.[225]

5.101 In some instances, overhead surveillance has been found to be a trespass. A person can bring an action in trespass for encroachments into the airspace above their land only to the extent that the encroachment affects their ordinary use and enjoyment of that land.[226] Therefore, while litigants have been able to sue for encroachment of billboards[227] and scaffolding,[228] they have been unable to do so in respect of overflight by aircraft.[229] Further, the *Wrongs Act 1958* (Vic) significantly limits a person's ability to bring an action for trespass or nuisance in respect of flight over land.[230]

5.102 A person may bring an action for nuisance to prevent persons from persistently conducting video surveillance of his or her property. In *Raciti v Hughes,* the court held that the behaviour of neighbour in setting up an elaborate system of bright lights and video cameras that recorded activities in the plaintiff's yard was a nuisance.[231]

5.103 Importantly, the actions for trespass and nuisance are of limited assistance, however, when considering the regulation of public place surveillance because they are relevant only when dealing with complaints made by owners of privately owned land.

5.104 By contrast, the action for breach of confidence has been used successfully in some high profile English cases[232] involving publication of material obtained by the use of surveillance in public places. The traditional action for breach of confidence, which provided a remedy when information originally communicated in confidence was disclosed, has been extended recently in the UK. This is probably due to the influence of the Human Rights Act and the European Convention on Human Rights and Fundamental Freedoms, to more closely resemble a tort of invasion of privacy.[233]

5.105 In *Campbell v MGN Ltd*[234]—a case concerning disclosure by a UK newspaper that model Naomi Campbell had attended a Narcotics Anonymous meeting—the House of Lords confirmed that the obligation to maintain the confidentiality of information no longer required the existence of a confidential relationship, but extended to a person who knows, or ought to know, that the information is confidential.[235] Lord Nicholls of Birkenhead said that the essence of the action for breach of confidence was misuse of private information.[236] The Victorian Court of Appeal recently referred to *Campbell* with approval when considering the remedies which may be ordered in an action for breach of confidence.[237]

5.106 Members of the Australian High Court have expressed similar views to those advanced in *Campbell* about the breadth of the action for breach of confidence. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (*Lenah Game Meats*),[238] Chief Justice Gleeson said that the obligations of confidentiality may arise even though 'there is no imparting of information in circumstances of trust and confidence…The nature of the information must be such that it is capable of being regarded as confidential.'[239]

5.107 A court may find that information obtained through surveillance is confidential in nature. As Chief Justice Gleeson said in *Lenah Game Meats*, '[a] photographic image, illegally or improperly or surreptitiously obtained, where what is depicted is private, may constitute confidential information'. The former Chief Justice referred to comments made by Justice Laws in *Hellewell v Chief Constable of Derbyshire*[240] with approval:

> *If someone with a telephoto lens were to take from a distance and with no authority a picture of another engaged in some private act, his subsequent disclosure of the photograph would, in my judgment, as surely amount to a breach of confidence as if he had found or stolen a letter or diary in which the act was recounted and proceeded to publish it. In such a case, the law would protect what might reasonably be called a right of privacy, although the name accorded to the cause of action would be breach of confidence.*[241]

5.108 The reach of the cause of action is unclear because the judgments do not indicate what type of 'private acts', in private or public places, would amount to a breach of confidence. Further, as the action for breach of confidence provides a remedy only for the wrongful disclosure of information, it does not protect against any surveillance activity that does not result in publication.

219 John Fleming, *The Law of Torts* (9th ed, 1998) 665.

220 See *Giller v Procopets* [2008] VSCA 236 for discussion of the available remedies.

221 *Grosse v Purvis* [2003] QDC 151; *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281.

222 See *Hosking v Runting* [2003] 3 NZLR 285 (New Zealand) and W Page Keeton et al, *Prosser and Keeton on Torts* (5th ed, 1984) (discussing recognition by state courts in the United States) 851.

223 It is an indirect protection because unlike a statute prohibiting some forms of surveillance, the action for trespass or the action for nuisance require that individuals show some harm and bring the matter before a court.

224 An action for trespass requires showing that there was a direct interference with the plaintiff's land; an action for nuisance requires showing some indirect interference with the plaintiff's right to use and enjoy their land. Danuta Mendelson, *The New Law of Torts* (2007) 117 and 529.

225 *Lincoln Hunt (Aust) Pty Ltd v Willesee* (1986) 4 NSWLR 457.

226 See *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] 1 QB 479, cited with approval in *LJP Investments Pty Ltd v Howard Chia Investments (No 2)* (1989) 24 NSWLR 490.

227 *Kelsen v Imperial Tobacco Co* [1957] 2 QB 344.

228 *LJP Investments Pty Ltd v Howard Chia Investments (No 2) (1989)* 24 NSWLR 490.

229 *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] 1 QB 479.

230 Section 30 of the *Wrongs Act 1958* (Vic) precludes such action 'by reason only of the flight of an aircraft over any property at a height above the ground which having regard to the wind the weather and all the circumstances is reasonable, or the ordinary incidents of such flight, so long as the provisions of the Air Navigation Regulations are duly complied with.' In general terms aircraft are required to maintain a minimum height of 1,000 feet above ground level over built up areas and 500 feet over all other areas: *Civil Aviation Regulations 1988* (Cth) regs 157 and 178.

231 *Raciti v Hughes* (1995) 7 BPR 14, 837. See also *Stoakes v Brydes* [1958] QWN 5; Peter Hutchesson (ed), *Khorasandjian v Bush* (1993) 143(6590) *New Law Journal* 329.

232 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457; *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.

233 *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB), [7] (Eady J).

234 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457.

235 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457, [14].

236 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457, [14].

237 *Giller v Procopets* [2008] 236. In that case the Court of Appeal was asked to consider the remedies available for breach of confidence rather than the conduct rendered unlawful by the cause of action.

238 (2001) 208 CLR 199.

239 (2001) 208 CLR 199, [34].

240 [1995] 1 WLR 804, 807.

241 (2001) 208 CLR 199, [34] (Gleeson CJ) citing *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, 807 (Laws J).

5.109 United Kingdom developments in this branch of the law were outlined recently in *Mosley v News Group Newspapers Limited*,[242] a highly publicised case involving publication of material about car-racing identity Max Mosley. In that case, Justice Eady found there had been a breach of confidence, and also noted that since the *Campbell* case, it is now

> *common to speak of the protection of personal information in this context, without importing the customary indicia of a duty of confidence.*[243]

However, Justice Eady concluded that only the House of Lords could decide whether this expanded cause of action (originally for breach of confidence) had in fact become a tort of privacy.[244]

INVASION OF PRIVACY: AN EMERGING CAUSE OF ACTION

5.110 The High Court of Australia has not yet recognised a tort of invasion of privacy. A tort of this nature would indirectly regulate some public place surveillance activities, particularly the use that could be made of information obtained by surveillance. This tort exists in a number of other common law countries, including New Zealand, the United States and Canada.[245] As we have seen, it is also emerging in the UK through an expanded action for breach of confidence.[246]

5.111 In 2002 the High Court removed an important impediment to the development of this tort in Australia by indicating that, contrary to some views, an earlier decision of the Court[247] did not 'stand in the path' of its development.[248]

5.112 Many of the judgments in *ABC v Lenah Games Meats Pty Ltd*[249] cautiously supported the development of a tort of invasion of privacy. Chief Justice Gleeson said that '[t]he law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy.'[250] Justices Gummow and Hayne said that while there were no impediments to the development of a tort, its existence was still open to question. They suggested that any new tort might fall within a group of existing legal and equitable wrongs drawn from 'a principle protecting the interests of the individual in leading, to some reasonable extent, a secluded and private life…"free from the prying, eyes, ears and publications of others"'.[251] Justice Callinan suggested that 'the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country'.[252]

5.113 Some of High Court Justices identified difficulties that might arise when developing a tort of invasion of privacy. Chief Justice Gleeson referred to the lack of precision in the concept of privacy, and to the tension that exists between the interests in privacy and the interests in free speech.[253] Justices Gummow and Hayne also commented on the lack of precision in the concept of privacy, acknowledging that 'the difficulties in obtaining in this field something approaching definition rather than abstracted generalisation have been recognised for some time'.[254]

5.114 Since the High Court's decision in *Lenah Game Meats*, trial courts in Queensland and Victoria have recognised a tort of invasion of privacy. In *Grosse v Purvis*[255] a judge in the Queensland District Court concluded that a prolonged course of stalking and harassment was an invasion of the plaintiff's privacy. The Court decided that the conduct in question was unlawful because it was characterised by the essential elements of the 'actionable right of an individual person to privacy'.[256] The court determined that the essential elements of an action for invasion of privacy are: an act performed by the defendant which intrudes upon the privacy of the plaintiff in a manner which would be considered 'highly offensive to a reasonable person of ordinary sensibilities', because it caused the plaintiff 'detriment in the form of mental, psychological, emotional harm or distress' or because it prevented or hindered her from doing an act which she was lawfully entitled to do.[257]

5.115 In *Jane Doe v Australian Broadcasting Corporation*,[258] Judge Hampel of the Victorian County Court ruled that an ABC radio news broadcast identifying a woman who had been attacked and raped by her estranged husband was a breach of privacy. The news broadcast contravened a statutory provision which made it an offence to publish information identifying a victim of a sexual offence by disclosing the name of the victim.[259]

5.116 Judge Hampel decided that it was not necessary to formulate an exhaustive definition of privacy and held that the wrong done was 'the publication of personal information, in circumstances where there was no public interest in publishing it, and where there was a prohibition on its publication.'[260] The plaintiff received a substantial award of damages for overlapping causes of action for breach of statutory duty, negligence and breach of privacy.[261] The decision has not been considered by an appeal court because the case was settled.

5.117 It may be useful for the courts when following the lead given by Chief Justice Gleeson 'to identify and protect interests of a kind which fall within the concept of privacy' to reflect upon the differences between the notions of *confidentiality* and *privacy*. Mendelson has written:

> *Confidentiality and privacy are quite different concepts, with separate histories and contexts. The concept of confidentiality, classically attached to interpersonal communications, defines rights and obligations of the two parties to a relationship. Privacy relates less to interpersonal communications and more to the scope and limits of individual autonomy.*
>
> *Whereas the legal concept of confidentiality reflects notions of trust embedded in the Judeo-Christian moral and ethical heritage, the concept of privacy—in the sense of a personal privilege to exclude others—is based on a social and legal distinction between intimate and public domains.*[262]

CREATING A PRIVACY CAUSE OF ACTION BY STATUTE

5.118 In lieu of recognition by the courts of a tort for invasion of privacy, parliament could create a privacy cause of action by statute. In 2008 the ALRC proposed creation of a statutory cause of action for invasion of privacy.[263] The ALRC's model builds on that suggested by the New South Wales Law Reform Commission (NSWLRC) in 2007.[264]

5.119 The NSWLRC provided a number of arguments in favour of introducing a statutory cause of action in NSW. These included the current lack of broad protection of privacy in civil law; the perceived and actual increasingly invasive social environment; Australia's obligations to protect privacy rights under international instruments;[265] and the development of more general privacy protections in overseas jurisdictions.[266]

5.120 The models proposed by the NSWLRC and ALRC provide for a general cause of action for invasion of privacy, along with a non-exhaustive list of the circumstances that could give rise to the cause of action.[267] The circumstances include an individual who has been subjected to 'unauthorised surveillance'.[268]

THE VICTORIAN CHARTER OF HUMAN RIGHTS AND RESPONSIBILITIES

5.121 The *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter) makes it unlawful for public authorities[269] to act in a way that is incompatible with the human rights listed in the Charter.[270]

242 *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB).

243 *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB), [181] (Eady J).

244 *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB), [184] (Eady J).

245 See the discussion later in this chapter about the regulation of surveillance practices in other countries.

246 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457.

247 *Victoria Park Racing and Recreation Grounds Company Limited v Taylor* (1937) 58 CLR 479.

248 See discussion at *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 249 [107]–[108].

249 (2002) 208 CLR 199.

250 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 225 [40].

251 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 258 [132] citing *Restatement of Torts,* 2d, §652A, Comment *b*.

252 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 328–9 [335].

253 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 225–6[41].

254 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 199, 252 [116].

255 [2003] QDC 151.

256 *Grosse v Purvis* [2003] QDC 151 [442].

257 *Grosse v Purvis* [2003] QDC 151 [444].

258 [2007] VCC 281.

259 *Judicial Proceedings Reports Act 1958* (Vic) s 4(1A).

260 [2007] VCC 281, [163].

261 The total damages awarded was $234,190: *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281, [194].

262 Danuta Mendelson, *The New Law of Torts* (2007) 152.

263 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008).

264 NSW Law Reform Commission, *Invasion of Privacy* Consultation Paper 1 (2007).

265 Including the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) and the *Universal Declaration of Human Rights*, GA res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN doc A/RES/217 A (III) (10 December 1948).

266 Including the United Kingdom, Canada and New Zealand. See NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007) 11–16

267 Ibid 153–155, 158; *Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report 108* (2008) 2584 (Recommendation 74-1–74-2).

268 *Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report 108* (2008) 2584 (Recommendation 74-1).

269 The term 'public authority' is defined broadly in the *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 4. It includes police, local councils and private entities that have functions of a public nature.

270 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38(1).

Chapter 5 Current Law

5.122 Individuals affected by such unlawful activities cannot take action under the Charter unless they have an existing basis, or cause of action, for challenging the unlawful activity.[271] For example, in *Sabet v Medical Practitioners Board of Victoria* (*Sabet*) a doctor sought review in the Supreme Court of Victoria of the Medical Practitioners Board's suspension of his medical registration. He argued that the action was unlawful because of the Board's failure to consider the presumption of innocence, a right under section 25(1) of the Charter.[272] He was able to mount this argument because he had a cause of action under the *Administrative Law Act 1978* (Vic) and grounds for review, including that the Board failed to take proper account of relevant considerations.[273]

5.123 The Charter right of most relevance to public place surveillance is the right to privacy in section 13. Section 12, which deals with the right to freedom of movement, is also relevant.[274] The wording of the right to privacy in section 13 is in almost identical to Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR).[275] Indeed, the drafters of the Charter modelled the human rights listed in the Charter primarily on the ICCPR,[276] a treaty to which Australia is a party.[277]

5.124 There has not been any judicial consideration of the scope of the right to privacy in section 13 of the Charter. However, since section 13 is modelled on the equivalent provision in the ICCPR, the scope of the right to privacy under that treaty is clearly relevant. The United Nations Human Rights Committee (the Human Rights Committee), the body charged with monitoring implementation of the ICCPR,[278] has recognised that the right to privacy may be breached through surveillance practices. For example, it has treated telephone tapping and interferences with the correspondence of prisoners as affecting the right to privacy.[279] In addition, a United Nations special rapporteur recently concluded that a program of secret surveillance in the United States was an interference with the right to privacy.[280]

5.125 Likewise, the European Court of Human Rights has imposed sanctions upon numerous countries for failing to regulate wiretapping by governments and private individuals[281] based on the right to privacy under Article 8 of the *European Convention on Human Rights*[282] (the European Convention). The provisions of the European Convention are similar to those of the ICCPR.[283] Decisions made under the European Convention are clearly relevant when determining the scope of the right to privacy in the Charter.

5.126 Public place surveillance may interfere with the right to privacy contained in the European Convention. In *PG and JH v United Kingdom*, the European Court concluded that covert recordings of suspects at a police station (not traditionally viewed as a private place) interfered with their right to privacy.[284] The Court came to this conclusion on the basis that there was 'a zone of interaction of a person with others, *even in a public context*, which may fall within the scope of "private life"' as the term is used in Article 8 of the European Convention (emphasis added).[285]

5.127 The European Court has also found invasions of privacy in other public contexts, including telephone calls on business premises,[286] publication of photographs of a celebrity 'practicing sport, out walking, leaving a restaurant or on holiday',[287] and television broadcast of CCTV street footage.[288] The latter is a reference to *Peck v United Kingdom*, where the applicant alleged a violation of Article 8 due to a local council's release to the media of CCTV footage of him attempting suicide, from which his friends and family were able to recognise him.[289] The court concluded that there had been a violation of his right to privacy, noting the failure of the council to take precautions, such as masking his image and obtaining his consent.[290]

5.128 Draft Guidelines prepared by the Victorian Department of Justice (DOJ Draft Guidelines)[291] to assist with implementation of the Charter identify public place surveillance as a possible 'policy trigger' for consideration of the right to privacy. Two forms of surveillance are listed:

- surveillance of persons for any purpose (such as CCTV)
- surveillance or other monitoring where recorded personal information is collected, accessed, used or disclosed.[292]

INSTANCES OF PUBLIC PLACE SURVEILLANCE THAT MAY VIOLATE THE CHARTER

5.129 Section 13 of the Charter prohibits only unlawful and arbitrary interferences with the right to privacy. When interpreting the similarly worded provision of the ICCPR, the Human Rights Committee, has said that the prohibition on unlawful interferences with the right to privacy means 'no interference can take place except in cases envisaged by the law'.[293] The requirement that interference not be arbitrary means that, in addition to being lawful, any interference must be in accordance with the provisions, aims and objectives of the treaty, and be reasonable in the particular circumstances.[294] By 'reasonable', the Committee means the interference must be proportionate to the end sought and necessary in the circumstances.[295]

5.130 In addition to prohibiting unlawful and arbitrary interferences with the right to privacy, the Charter requires that any limitation on a right contained in the Charter meet the requirements set out in section 7(2), the 'general limitations clause'. That section states:

> *A human right may be subject under law only to such reasonable limits as can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom, and taking into account all relevant factors including:*
>
> *(a) the nature of the right; and*
> *(b) the importance of the purpose of the limitation; and*
> *(c) the nature and extent of the limitation; and*
> *(d) the relationship between the limitation and its purpose; and*
> *(e) any less restrictive means reasonably available to achieve the purpose that the limitation seeks to achieve.*[296]

The section was modelled on human rights legislation in Canada, New Zealand and South Africa which contain a similar limitations clause.[297]

5.131 In order to demonstrate that surveillance is reasonable, the DOJ Draft Guidelines suggest that a public authority conducting surveillance must show that the needs of the state in the particular instance outweigh the rights of individuals.[298] The standard is high, with the state needing to show that 'the exercise of the human right would be "inimical to the realisation of collective goals of fundamental importance"'.[299]

5.132 To show that the surveillance is demonstrably justified in a free and democratic society,[300] the public authority would need to demonstrate that the

271 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 39(1). Moreover, the Charter requires courts, tribunals and others who interpret and apply the law to interpret all Acts and subordinate instruments (whether passed before or after the Charter's commencement) in a way that is compatible with human rights. *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 32; and Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) Section 1. In addition, the Charter requires that members of parliament when proposing new legislation prepare a statement setting out whether it is compatible with human rights, and if so, how it is compatible, and if it is not compatible, the nature and extent of the incompatibility. *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 28.

272 [2008] VSC 346, [3], [102].

273 [2008] VSC 346, [3], [104].

274 Draft Guidelines suggest that surveillance which enables a public authority to monitor or trace the movements of a person within Victoria should act as a policy trigger for consideration of the right to freedom of movement. Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) section 12.

275 United Nations, International Covenant on Civil and Political Rights Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966: entry into force 23 March 1976, in accordance with Article 49 . Section 13 of the Charter defines the right to privacy as the right of a person 'not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with'. Article 17 of the ICCPR states in part: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence …'

276 Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) Section 1.

277 Note however that the provisions of a treaty to which the country is a party are enforceable in Australian courts only after parliament has enacted implementing legislation. *Minister of State for Immigration and Ethnic Affairs v Teoh* (1995) 183 CLR 273, 286-287. A number of Australian laws partially implement the right to privacy found in the ICCPR. For example, the *Privacy Act 1988* (Cth) implements the right to privacy in the ICCPR with respect to the activities of Commonwealth government agencies and some private sector organisations, and their handling of personal information.

278 *Introduction to the Human Rights Committee,* Office of the High Commissioner for Human Rights <www.unhchr.ch/html/menu2/6/a/introhrc.htm> at 7 July 2008.

279 Sarah Joseph, et al, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (2nd ed) (2004) 492.

280 United Nations, 'Preliminary Findings on Visit to United States by UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (Press Release, 29 May 2007) <www.unhchr.ch/huricane/huricane.nsf/view01/338107B9FD5A33CDC12572EA005286F8?opendocument> at 2 July 2008.

281 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007) 7 citing *Klass v Germany* (1978) 28 Eur Court HR (ser A) and *Malone v Commissioner of Police* (1979) 2 All ER 620.

282 Article 8(1) of the European Convention states: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11*, opened for signature 4 November 1950 ETS 5 (entered into force 1 November 1998) <www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf> at 2 July 2008.

283 See Manfred Nowak, *U N Covenant on Civil and Political Rights: CCPR Commentary* (2nd revised ed) (2005) XXIII (noting reliance by drafters of the European Convention on the Human Rights Commission's drafts of the ICCPR) and XXVI (stating that interpretation of the ICCPR can be aided by similar regional treaties such as the European Convention).

284 *PG and JH v United Kingdom* 44787/98 [2001] IX Eur Court HR [52], [60].

285 *PG and JH v United Kingdom* 44787/98 [2001] IX Eur Court HR [56].

286 *Halford v United Kingdom* 20605/92 [1997] III Eur Court HR [44],[46].

287 *Von Hannover v Germany* 59320/00 [2004] VI Eur Court HR [61].

288 *Peck v United Kingdom* 44647/98 [2003] I Eur Court HR.

289 *Peck v United Kingdom* 44647/98 [2003] I Eur Court HR [21].

290 *Peck v United Kingdom* 44647/98 [2003] I Eur Court HR [80].

291 Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) section 13.

292 Ibid section 13.

293 United Nations, *Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies* HRI/GEN/1/Rev.7 (2004) 142 [3].

294 Ibid 142 [4].

295 *Toonen v Australia*, Human Rights Committee, Communication no 488/1992, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) [8.3].

296 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 7(2).

297 Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) section 2.2.

298 Ibid section 2.

299 Ibid section 2 citing the Canadian Supreme Court case *R v Oakes* [1986] 1 SCR 103.

300 Ibid. Section 7 of the Charter is based in part on the test developed by the Court in that case and known as 'the Oakes test'.

limitation on privacy 'is justified in the circumstances'.[301] This requires presenting material, including studies, reviews, inquiries and consultation findings.[302] The Draft Guidelines also suggest that:

- the purported purpose of the surveillance must at minimum be a societal concern that is pressing and substantial in a free and democratic society, and this is more than just an effort to achieve a common good;[303] and
- the purpose of surveillance would need to relate to an area of public or social concern that is important, and not trivial.[304] Economic considerations alone (other than a serious fiscal crisis) will almost never be important enough to justify a limitation to a right.[305]

5.133 Two opinions of the European Commission for Democracy Through Law (Venice Commission)[306] in relation to the European Convention provide some useful guidance about types of surveillance that might or might not constitute an acceptable limitation on the right to privacy under the Charter.[307] The opinions are particularly relevant as Article 8(2) of the European Convention is similar to the general limitations clause of the Charter for it requires that an interference be 'necessary in a democratic society'.[308] According to the European Court, the requirement that an interference with privacy be 'necessary in a democratic society' is in part an inquiry into proportionality between means and ends.[309]

5.134 The Venice Commission has said with respect to public sector surveillance that: 'a disproportionate measure would be, for instance, to use video-surveillance devices in public toilets to control and maintain a non-smoking policy in this area.'[310] It has also commented on widespread and indiscriminate use of public place surveillance, saying:

> *the aim to prevent the commission of crimes cannot, apart from exceptional situations of imminent threats to security or risks of serious crimes, justify an a-selective surveillance system that implies far-going limitations of privacy and movement for the public at large, since it may be assumed that more selective systems of surveillance are available and sufficiently effective.*[311]

5.135 The Venice Commission has identified a number of requirements for video surveillance by public authorities and private users of public surveillance when seeking to ensure that surveillance is a proportionate response to potential harm:

Public Authorities

- People should be notified if they are being watched in public places, or else the surveillance system should be obvious;
- People subject to surveillance should have an effective remedy if they believe their rights have been infringed; they must also be informed of the remedy and how to use it;
- Personal data resulting from the surveillance should be obtained and processed fairly and lawfully;
- Personal data should be collected for a specified and legitimate purpose and relevant and not excessive in relation to the purpose;
- Personal data should not be used in ways incompatible with the purpose for which it was collected;
- Personal data should be accurate and, where necessary, kept up to date;
- Personal data should be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which it is stored;
- Personal data should be available for access by the individuals to which it relates, subject to restrictions which balance their rights against the need to restrict access for the purpose of prevention and prosecution of crime, and the privacy interests of third parties; and
- The video surveillance measures should be supervised by an independent authority.[312]

Private users of surveillance

- The relevant public place under surveillance should be closely adjacent to the private area the person wants to protect; thus surveillance must not cover larger parts of the street than necessary or be installed such as to cover the exterior or interior of other houses;
- A person entering another's property where there is surveillance should be informed or made aware of the surveillance or its possibility; and is entitled to know if data has been collected and how it will be processed or used; and
- That person should also have a legal remedy entitling them to have the legality of the surveillance reviewed.[313]

Camera surveillance in shops

- Cameras may be justified to protect property if proven to be necessary and proportionate; and
- Cameras may be justified in certain locations to prevent and prosecute robberies only if proven necessary, and for no longer than necessary.[314]

WHEN CHARTER HUMAN RIGHTS CONFLICT

5.136 There may sometimes be conflict between Charter rights because protecting one person's rights may limit those of another. For example, while the use of a surveillance device may interfere with the right to privacy, that activity may also be an exercise of the right to freedom of expression set out in section 15 of the Charter.[315]

5.137 The general limitations clause in section 7(2) of the Charter is designed to assist in resolving conflict between human rights. For example, in determining if the right to privacy can be reasonably limited in order to exercise the right to freedom of expression, it would be necessary to consider the importance of the right to freedom of expression in that context and whether the right was actually being advanced by the interference with privacy rights.[316]

NON-BINDING GUIDELINES, STANDARDS AND POLICIES

5.138 Because there are few laws that regulate surveillance in public places, most users of surveillance must look to advisory guidelines and industry standards, or devise internal policies and procedures, in order to provide the people responsible for surveillance activities with some guidance about practices that are permissible and those that are unacceptable. 'Rules' of this nature may be of limited effect because they are not subject to external oversight and enforcement. The level of compliance—and, therefore, the level of privacy protection for members of the public—is likely to vary according to the individual user.

5.139 The terms codes, guidelines, standards and policies are often used interchangeably. To avoid confusion, we have taken an approach that is consistent with the way language is used in the Privacy Act (Cth) and in the ALRC Privacy report, therefore:

- 'Binding codes' are the enforceable legislative agreements set up under the Privacy Act, as discussed above.
- 'Guidelines' are designed for the interpretation of legislation, and are usually issued by government departments.
- 'Voluntary standards' are developed, for example, by a peak body or at an industry level, and may not only reflect the application of the law, but also incorporate 'best practice' principles for surveillance use.
- 'Internal policies and procedures' are developed at an individual business level.

301 Ibid section 2.

302 Ibid section 2.

303 Ibid section 2.

304 Ibid section 2.

305 Human Rights Unit, DOJ [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) section 2.

306 The Venice Commission is the Council of Europe's advisory body on constitutional matters.

307 European Commission for Democracy for Law (Venice Commission), *Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights* study no 404 (2007) <www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf> at 4 July 2008; and European Commission for Democracy for Law (Venice Commission), *Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection: Adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007)* CDL-AD(2007)027 (2007) <www.venice.coe.int/docs/2007/CDL-AD(2007)027-e.asp> at 4 July 2008.

308 Article 8(2) states: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.' *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No 11*, opened for signature 4 November 1950 ETS 5 (entered into force 1 November 1998) <www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf> at 2 July 2008.

309 *Peck v United Kingdom* 44647/98 [2003] I Eur Court HR [76].

310 European Commission for Democracy through Law (Venice Commission), *Opinion on Video Surveillance in Public Places By Public Authorities and the Protection of Human Rights* (2007) [65] <www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf> at 4 July 2008.

311 Ibid 66.

312 Ibid [73]–[78].

313 European Commission for Democracy Through Law (Venice Commission), *Opinion: On Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection* (2007) [49]–[50] <www.venice.coe.int/docs/2007/CDL-AD(2007)027-epdf at 4 July 2007.

314 Ibid [57]

315 'Every person has the right to freedom of expression which includes the freedom to seek, receive and impart information and ideas of all kinds, whether within or outside Victoria': *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 15(2). Like the right to privacy, the right of freedom of expression is subject to qualifications, including that it "may be subject to lawful restrictions reasonably necessary … to respect the rights and reputation of other persons": *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 15(3)(a).

316 Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Draft Guidelines for Legislation and Policy Officers in Victoria* (2006) section 2.2.

Chapter 5 Current Law

GUIDELINES

5.140 The Privacy Act (Cth) empowers the Federal Privacy Commissioner to issue advisory guidelines about the application of privacy law. Most of the published guidelines have no relevance to public place surveillance. A notable exception is the Commissioner's guidelines for covert surveillance by Commonwealth agencies.[317] Those guidelines stipulate that covert optical surveillance should be undertaken only for a lawful purpose related to an agencies functions; that approval for the surveillance be given at a senior level; that it be undertaken only if other forms of investigation are not suitable; and that the benefits of obtaining information from surveillance substantially outweigh the privacy intrusion of the surveillance subject. The guidelines also include specific guidance for agencies conducting covert surveillance to investigate disputed compensation claims.

5.141 The Victorian Privacy Commissioner has developed information sheets in relation to some aspects of public place surveillance, including mobile telephones with cameras,[318] GPS,[319] and captured images.[320] The Commissioner has also considered the application of the information privacy laws in the context of transport sector surveillance.[321] While not binding in any way, these documents provide useful discussion of the privacy implications of these types of surveillance devices, and policy measures to prevent their abuse. The Commissioner has also provided a number of information sheets and guidelines in relation to privacy generally, [322] which are relevant to users of public place surveillance.

5.142 The Victorian Department of Infrastructure (DOI) (now the Department of Transport) has *Policy and Procedures for the Management of CCTV Evidence Records* in place to ensure that surveillance footage is able to be used as evidence in court (known as the 'Keeper of Evidence' process).[323] Under their franchise agreements, train operators in Victoria must provide CCTV images of incidents occurring on the transport systems to the Keeper of Evidence, a designated person within the DOI.[324] The policy includes 'principles' to be followed in relation to collected CCTV data.[325] It also outlines processes by which CCTV footage may be released to members of the public, Victoria Police and other stakeholders.[326]

5.143 Guidelines for compliance with legislation have also been developed at an industry level. For example, the Australian Institute of Petroleum and the police have developed national guidelines for petrol service station use of surveillance cameras.[327] The guidelines note that privacy or surveillance devices legislation restricts how video and audio surveillance can be undertaken, and states that in general, the law requires that surveillance be clearly brought to the attention of staff and customers.[328] The guidelines also state that there should be no surveillance in washrooms, toilets, change rooms, and other areas where staff and customers can reasonably expect privacy, and that surveillance footage should not be disclosed to third parties, such as the police, unless there is a legitimate reason to do so.[329]

VOLUNTARY STANDARDS

5.144 The *National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* was approved by the Council of Australian Governments (COAG) in 2006[330] following the Madrid and London train bombings.[331] The code, which applies to specified forms of mass public transport including trains, trams and buses,[332] covers quality standards of surveillance systems and permissible uses and disclosure of surveillance footage for counter-terrorism purposes.[333] The code is not mandatory, but is 'designed to guide possible future investments in CCTV'.[334] It establishes different requirements for different facilities, with the highest level being for surveillance systems capable of identifying a person or object, and the lowest level simply requiring observation of the general area.[335] The code includes a recommended community consultation approach to camera location and installation.[336]

5.145 The Department of Justice has developed a *CCTV Toolkit for Victoria*. It is an information tool to assist local government users in deciding whether to install a CCTV system.[337] The toolkit recommends a seven-step process for evaluating the usefulness of a proposed CCTV system.[338] For example, steps one and two involve determining a crime prevention strategy and establishing how CCTV would contribute to that strategy.[339] In terms of privacy,

the toolkit recommends that local government consult with civil liberty groups and others who are interested in ensuring the CCTV system chosen 'does not impinge upon rights, such as individuals' general right to privacy'.[340] The toolkit contains recommendations only; it is not binding on anyone who uses it.[341]

5.146 The Australian Retailers Association has issued voluntary standards for Australian retailers about the use of RFID tags.[342] These have been developed to 'protect the interests of consumer privacy in the operation of RFID networks'.[343] The voluntary standards prescribe that retailers must, among other things, give clear notice of the presence of RFID tags on products; educate consumers about RFID technology; provide details of the retention, use and security of collected data; and provide consumers with the choice to discard, remove or disable a RFID tag on an item they have purchased.[344]

5.147 Some industry bodies specifically recommend the use of CCTV or other surveillance devices. For example, we were informed that the Pharmacy Guild of Australia's policy is to recommend that pharmacies have CCTV to prevent shoplifting.[345] Additionally, new taxi security camera standards, currently being developed by DOI, will establish a minimum benchmark for camera specification and performance.[346] New cameras will be installed in taxis operating in Victoria from January 2009.[347]

5.148 Some standards developed by official standards bodies also relate to public place surveillance. There is an Australian Standard regulating the management and operation of CCTV systems in public places.[348] The standard is designed to cover CCTV systems used in areas where 'the public is encouraged to enter or have a right to visit' including town centres, shopping centres and public transport.[349] Its section on privacy states that cameras should not be used to infringe the individual's privacy rights and specifically addresses issues such as avoiding filming the interior of private properties, removing identifying information relating to third parties (such as by masking identifying number plates) when exporting data relating to intruders and confining uses of CCTV systems to the purposes intended.[350] The standard also contains detailed guidance regarding permitted disclosures to third parties (such as police) and obligations to provide access to data subjects.[351]

INTERNAL POLICIES

5.149 Many users of surveillance in public places told the commission during consultations that they follow internal policies and practices in order to limit privacy invasion. For example, local council policy manuals on CCTV cover various aspects of surveillance, including how CCTV is to be used and

317 Office of the Federal Privacy Commissioner and Human Rights and Equal Opportunity Commission, *Covert Surveillance in Commonwealth Administration: Guidelines* (1992).

318 Office of the Victorian Privacy Commissioner, *Mobile Phones with Camera*s Info sheet 05.03 (2003).

319 Office of the Victorian Privacy Commissioner, *Privacy and Global Positioning System Technology*, Info Sheet 02.08 (2008).

320 Office of the Victorian Privacy Commissioner, *Images and Privacy,* Info Sheet 01.03 (2003).

321 Office of the Victorian Privacy Commissioner, *Victorian Taxi and Tow Truck Directorate: Surveillance Cameras in Taxis: Report of Findings* Privacy Audit 01.06 (2006); and Privacy Victoria, *Submission to the Transport Legislation Review* (14 December 2007) <www.privacy.vic.gov.au/dir100/PriWeb.nsf/download/52881783E99648BACA2573D80080D79D/$FILE/OVPC%20submission%20Transport%20Legislation%20Review%2014.12.07.pdf> at 11 June 2008.

322 See, eg, Office of the Victorian Privacy Commissioner, *Who's covered by the Information Privacy Act?*, Info Sheet 01.06 (2006); Office of the Victorian Privacy Commissioner, *Short Guide to the Information Privacy Principles* (2006); Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines Edition.01 (2006).

323 Department of Infrastructure, *Policy and Procedures for the Management of CCTV Evidence Records* (2007). The commission notes that this document is no longer available on the Department's website.

324 Department of Infrastructure, *Public Transport Partnerships: An Overview of Passenger Rail Franchising in Victoria* (2005) 74.

325 Department of Infrastructure, *Policy and Procedures for the Management of CCTV Evidence Records* (2007) 10 – 12.

326 Ibid 13–15.

327 Roundtable 20.

328 Australian Institute of Petroleum, *Guidelines: Service Station Security* (2002) 16 <www.aip.com.au/pdf/sss_guide.pdf> at 27 June 2008.

329 Ibid.

330 Council of Australian Governments, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (2006).

331 Ibid .

332 Ibid .

333 Roundtable 12.

334 Council of Australian Governments, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (2006) 6.

335 Roundtable 12.

336 Roundtable 12.

337 Department of Justice, Victoria, *CCTV Toolkit for Victoria: Is CCTV the Best Response?* (2007). The commission notes that this document is no longer available on the Department of Justice website.

338 Ibid 2.

339 Ibid 4–7.

340 Ibid 9.

341 Ibid 2.

342 Australian Retailers Association, *Radio Frequency Identification (RFID) in Retail: Consumer Privacy Code of Practice* (2007).

343 Ibid 4.

344 Ibid.

345 Roundtable 15; and see, eg, *Pseudoephedrine-Related Break and Enter: 10 Practical Tips to Reduce Your Risks,* Pharmacy Guild of Australia (2007) 1 <www.guild.org.au/uploadedfiles/Qld_Branch/What's_New/Pharmacy%20Security_Final.pdf> at 23 January 2009.

346 See: Department of Infrastructure, *Action: The Victorian Taxi Safety Strategy: New Security Cameras for Victoria's Taxis* <www.transport.vic.gov.au/DOI/DOIElect.nsf/$UNIDS+for+Web+Display/40A969C6A7B911E4CA257332001B103B/$FILE/VTD%20Fact%20Sheet%20-%20New%20Security%20Cameras%20for%20Victoria's%20Taxis.pdf> at 26 November 2007.

347 Ibid.

348 Standards Australia, *Closed Circuit Television (CCTV): Part 1: Management and Operation*, AS 4806.1—2006 (2006).

349 Ibid 5.

350 Ibid 18.

351 Ibid 19-21.

shared with police.[352] As most of the local councils consulted worked in partnership with the police, sharing of surveillance footage was common. Some councils require police to formally apply for access to footage.[353] Generally, this involved providing valid reasons for requesting a copy of recorded footage.[354]

5.150 Council policies also include guidelines on antisocial behaviour response (including how to avoid profiling),[355] storage and collection practices in accordance with the IPA (Vic),[356] and requiring signage advising people that surveillance cameras are in operation.[357] One council has developed a policy document covering issues such as who has access to the Camera Control Centre where cameras are monitored, rules governing the liaison with police, and rules for sharing of footage.[358]

5.151 In consultations with the transport sector, we were advised that one operator has a privacy policy and a memorandum of understanding with DOI that determines its CCTV policy and guidelines on inappropriate filming.[359] In tram operations, policies are in place and management must approve any disclosure of footage.[360]

5.152 A large grocery chain has a national policy on the use of surveillance cameras in its stores. It includes prohibiting surveillance cameras in toilets, providing notice that surveillance is taking place, and logging of all CCTV footage provided to police. The store has also developed privacy guidelines, in consultation with the Privacy Commissioner, that it uses in employee induction and training.[361] Employees using surveillance inappropriately are subject to disciplinary action.[362]

5.153 Shopping centres also told the commission that they have internal policies and practices. For example, centres told the commission they will release CCTV footage only to police and insurers, and not to members of the public and the media.[363] In addition, police must make a written request for the footage.[364] A manager of a number of shopping centres in Victoria told the commission that his organisation has its own guidelines that require management's signature for CCTV footage download and release.[365] Employees who use CCTV inappropriately are subject to penalties.[366]

5.154 Banks also have their own standard practices.[367] For example, banks apply internal protocols and procedures for viewing, accessing and releasing CCTV footage. This includes requiring police to put requests for footage in writing, or when the bank is not itself the victim of crime, requiring a warrant for release of the footage.[368]

5.155 Sporting and entertainment venues rely on their own internal policies on surveillance. For example, one venue has a code of conduct.[369] Other sporting and entertainment venues told the commission they discipline employees for inappropriate use of surveillance, and a representative body for various clubs reported that misuse of surveillance systems can lead to dismissal.[370]

5.156 Some private businesses have internal policies concerning the use of surveillance. For example, a retailer has guidelines on the recording, retrieval and storage of surveillance materials. Its employee induction program includes materials stating that surveillance is not to occur in toilets and change rooms. The retailer authorises only certain individuals to operate surveillance cameras, and any misuse of cameras or surveillance materials is a dismissible offence.[371]

THE REGULATION OF PUBLIC PLACE SURVEILLANCE IN OTHER COUNTRIES

5.157 Public place surveillance is more directly regulated in some other countries than it is in Victoria and in other parts of Australia. This occurs by way of:

- specific provisions in information privacy laws and their application to surveillance through codes of practice or specific privacy law provisions
- specific legislation covering video surveillance in public places.

In addition, some countries have a right of action for invasion of privacy, either created through the courts or by legislation.

INFORMATION PRIVACY LAWS

5.158 In some countries information privacy laws regulate the use of surveillance in public places. Surveillance in public places falls within the scope of the laws, since video and sound recordings of individuals can constitute collection of personal information.[372]

5.159 The Netherlands is an example of a country relying on its information privacy laws to regulate public place surveillance. In the Netherlands, the Data Protection Authority has issued fact sheets clarifying the application of the Dutch data protection law to such surveillance. The fact sheets state, for example, that public authorities:

- can only use public surveillance where other measures have failed to reduce crime[373]
- camera surveillance must be used in conjunction with other measures, such as street lighting and manned surveillance.[374]

5.160 With respect to shopkeepers, the fact sheets state that they must:

- install notice of surveillance clearly at the entry to their premises[375]
- refrain from using cameras in changing rooms [376]
- use surveillance cameras only for protection of staff or property, and therefore install systems only in areas relevant to these activities, such as the entrance, shelves, or cash desks[377]
- hidden cameras in shops are not permitted unless there has been a high level of theft and other measures have not worked, and that such cameras must be temporary and not infringe on the privacy of customers and staff.[378]

The fact sheets also cover housing corporations, stating that they may use surveillance cameras to protect their property and their residents, but should not allow the systems to capture images of the street or front doors and windows of people's homes.[379]

5.161 The United Kingdom is another example of a country that has used its information privacy laws to regulate public place surveillance. The Information Commissioner has issued a *CCTV Code of Practice* which describes measures that must be taken to comply with the country's *Data Protection Act*.[380] The *Code* requires users of CCTV to do a number of things including:

- assess the appropriateness of using CCTV[381]
- establish clear procedures on how the CCTV system will be used[382]
- place cameras in order to capture only areas intended for monitoring[383]
- ensure that the system is not used to record conversations between members of the public 'as this is highly intrusive and unlikely to be justified'[384]
- in the case of a public authority user, assess whether CCTV is in response to a pressing need, is justified in the circumstances, and proportionate to the problem.[385]

352 Roundtables 7 and 8.
353 Roundtable 7.
354 Roundtable 7.
355 Roundtable 7.
356 Roundtable 7.
357 Roundtable 8.
358 *Safe City Cameras*, City of Melbourne <www.melbourne.vic.gov.au/info.cfm?top=183&pg=1299> at 7 July 2008.
359 Roundtable 23.
360 Roundtable 19.
361 *Privacy Policy,* Coles Group Limited (2006) <www.colesgroup.com.au/Home/privacy.asp> at 2 June 2008.
362 Roundtable 14.
363 Roundtable 31.
364 Roundtable 31.
365 Roundtable 31.
366 Roundtable 31.
367 Roundtable 29.
368 Roundtable 29.
369 Roundtable 13.
370 Roundtable 13.
371 Roundtable 15.
372 Article 29 Data Protection Working Party, European Commission, *Working Document on the Processing of Personal Data by Means of Video Surveillance* Adopted on 25 November 2002:11750/02/EN: WP 67 (2002). See also Office of the Federal Privacy Commissioner and Human Rights and Equal Opportunity Commission, *Covert Surveillance in Commonwealth Administration: Guidelines* (1992) 7; Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003) 3; and Office of the Victorian Privacy Commissioner, *Victorian Taxi and Tow Truck Directorate: Surveillance Cameras in Taxis: Report of Findings* Privacy Audit 01.06 (2006) 1.
373 College Bescherming Persoonsgegevens, *If You are Recorded by a Video Camera*, Fact Sheet No 20B (2005).
374 Ibid.
375 Ibid.
376 Ibid.
377 Ibid.
378 Ibid.
379 Ibid.
380 Information Commissioner's Office [UK], *CCTV Code of Practice* (revised ed, 2008) <www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf> at 13 January 2009.
381 Ibid 6-7.
383 Ibid 9.
384 Ibid 10.
385 Ibid 7.

Current Law

5.162 In the UK, there is also an *Industry Code of Practice: For the use of mobile phone technology to provide passive location services in the UK*. The code has been developed by industry rather than government.[386] Passive location services are those in which a mobile phone user consents to have his or her location tracked by another person, either from the other person's mobile phone or a computer.[387] In Chapter 2 we referred to parents tracking their children's movements via mobile phones. On the basis of the data protection legislation and other applicable laws,[388] the code requires, for example, that only the parent or guardian of a child under the age of 16 be able to track that child, that the service not be used for any form of unauthorised surveillance, and that the tracked individual be notified in writing and later through short message service (SMS) alerts that their location is being tracked.[389]

5.163 In Ireland, an advisory statement issued by the Data Protection Commissioner provides that under the *Irish Data Protection Act* 'all uses of CCTV must be proportionate and for a specific purpose'.[390] Further, as CCTV may infringe the privacy of the persons captured in the images, 'there must be a genuine reason for installing such a system'.[391] It explains that the requirement for proportionality means:

- in order for a business to install a camera in a toilet area (but not within cubical or urinal areas, where it is always inappropriate) it would need to demonstrate a frequent pattern of security breaches in that area
- cameras must be positioned so as not to capture non-relevant images in the vicinity.[392]

5.164 Canada regulates video surveillance in public through its *Privacy Act* (covering the public sector)[393] and through its *Personal Information Protection and Electronic Documents Act* (PIPEDA) (covering the private sector).[394]

5.165 In March 2008, the Office of the Privacy Commissioner of Canada issued *Guidelines for Overt Video Surveillance in the Private Sector* with the stated goal of helping organisations to achieve compliance with private sector privacy legislation.[395] The guidelines list '10 things to do when considering, planning and using video surveillance' including determining whether a less privacy-invasive means would be adequate, limiting the use and range of cameras as much as possible, and periodically evaluating the need for video surveillance.[396] The guidelines state that signs should be posted at the entry to premises because 'this gives people the option of not entering the premises if they object to the surveillance'.[397]

5.166 However, the Commissioner also took the view that notice provided to the public was insufficient, reasoning that the 'fundamental right to privacy cannot be extinguished simply by informing people that it is being violated.'[398] In the Commissioner's view, the cameras themselves threatened 'the privacy right of being "lost in the crowd," of going about our business without being *systematically* observed or monitored, particularly by the state.'[399]

5.167 In 2001 the Canadian Privacy Commissioner, who is responsible for investigating and resolving complaints under the *Privacy Act*, concluded that continuous video surveillance by the Royal Canadian Mounted Police (RCMP) of a street area, absent a specific incident related to law enforcement activity, was in breach of the Act.[400] The Commissioner stated

> *It is a tenet of the [Privacy] Act that an institution can collect only the minimum amount of personal information necessary for the intended purpose…There is no doubt that preventing or deterring crime can be regarded as an operating program or activity of the RCMP…[but] it does not follow that monitoring and recording the activities of vast numbers of law-abiding citizens as they go about their day-to-day lives is a legitimate part of any such operating program or activity.*[401]

5.168 In answering a complaint about the placement of cameras in the Canadian city of Yellowknife, the Privacy Commissioner concluded that a private security firm had breached information privacy laws when it installed video cameras on top of its office building, aimed at the city's main intersection. The use of the cameras involved the collection of information without consent of the individuals filmed, in contravention of the law.[402] Similarly, in 2002, the Commissioner concluded that a bank breached the law when it

released footage to the local media of a person it incorrectly believed had tried to cash a stolen cheque.[403] The Commissioner found that the bank took insufficient care to ensure the footage was accurate, because solving a crime requires a high degree of accuracy of information.

5.169 The New Zealand Police's *Policy on Crime Prevention Cameras in Public Places* proceeds on the basis that privacy laws apply to public surveillance.[404] For example, it states that the *Privacy Act 1993* requires that people from whom personal information is collected be made aware that information is being gathered about them, and the purpose for its collection. It further states that signs be posted at the location where cameras have been installed to notify the public that a camera is or may be operating. Also, the policy states that the Privacy Commissioner should be informed of any proposal to install new cameras or expand an existing scheme, and that the Commissioner should have the right to review the need for and use of cameras.

5.170 In some countries, data privacy laws contain specific provisions about video surveillance in public places. For example, section 6b of Germany's *Data Protection Act* (*Bundesdatenschutzgesetz* or *BDSG*) restricts the circumstances in which surveillance of public places by the use of video surveillance is lawful. The law, which applies to both public and private bodies, states:

> *The surveillance of publicly accessible spaces using opto-electronic equipment (video surveillance) shall be lawful only if it is necessary 1. for public bodies to discharge their duties, 2. for exercising control over a premises or 3. to protect legitimate interests for specifically stated purposes and there are no grounds for believing that there are overriding legitimate interests of the data subjects at stake.* [405]

5.171 According to one author, this and similar legislation at the state level in Germany has affected government use of public place surveillance, in that police have had to justify installation of CCTV.[406] Moreover, 'an installation will often be preceded by

386 *Industry Code of Practice: For the use of mobile phone technology to provide passive location services in the UK* (revised ed, 2006) 3 <www.followus.co.uk/LocationCodeJuly2006.pdf> at 19 January 2009.

387 Ibid.

388 Ibid 4.

389 Ibid 5-7.

390 Office of the Data Protection Commissioner, Ireland, '6.1 What Issues Surround the Use of CCTV?', *Frequently Asked Questions* <https://www.dataprotection.ie/viewdoc.asp?DocID=642> at 19 January 2009.

391 Ibid.

392 Office of the Data Protection Commissioner, Ireland, *Data Protection and CCTV* <http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/Documents/guidance/cctv.htm> at 19 January 2009.

393 *Privacy Act* RS C 1985 c P-21.

394 *Personal Information Protection and Electronic Documents Act* RS C 2000, c 5.

395 Office of the Privacy Commissioner of Canada, Guidelines for Overt Video Surveillance in the Private Sector (2008) 1 <http://www.privcom.gc.ca/information/guide/2008/gl_vs_080306_e.pdf> at 19 January 2009. Earlier, in 2006, the Canadian Privacy Commissioner issued guidelines on the use of video surveillance by police and law enforcement in public places: Office of the Privacy Commissioner of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (2006) <http://www.privcom.gc.ca/information/guide/vs_060301_e.asp> at 19 January 2009.

396 Ibid 2.

397 Ibid 3.

398 George Radwanski, Privacy Commissioner of Canada, *Privacy Commissioner's Finding on Video Surveillance by RCMP in Kelowna* (2001) Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/cf-dc/pa/2001-02/02_05_b_011004_e.asp> at 4 December 2007.

399 Ibid (emphasis in original).

400 Ibid.

401 Ibid.

402 Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #1: Video surveillance activities in a public place* (2001) <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010615_e.asp> at 19 January 2009.

403 See *Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #53: Bank accused of providing police with surveillance photos of the wrong person* (2002) <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020628_1_e.asp> at 19 January 2009.

404 See Rob Robinson, Commissioner of Police, New Zealand, *Policy on Crime Prevention Cameras in Public Places* (2003) <http://www.police.govt.nz/resources/2003/cctv/> at 19 January 2009.

405 *Bundesdatenschutzgesetz* [Federal Data Protection Act] *1990* (Germany) s 1; letter from Susanne Bohn, Der Bundesbeauftragte fur den Datenschutz und die Informationsfreiheit [Federal Commission for Data Protection and Freedom of Information [Germany]] to Victorian Law Reform Commission, 28 November 2008. Note however that while there are some general provisions, there are also parts of the Act which apply to the public sector and the private sector differently: see *Bundesdatenschutzgesetz* [Federal Data Protection Act] *1990* (Germany) pt II (public bodies) and pt III (private bodies).

406 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 221.

a crime rate analysis to prove the need for CCTV and this analysis will continue whilst the cameras are in action'.[407] In the view of this author, the provision has also limited CCTV use more generally in Germany:

> *it is safe to say that so far the legal requirements have lead to police and decision makers being cautious about the installation of CCTV. This is reflected in the relative* [sic] *limited number and size of CCTV systems in Germany (which usually consist of less than 10 cameras) and the fact that in Leipzig one camera was dismantled after it was deemed no longer…necessary.*[408]

5.172 Norway's *Personal Data Act*[409] and subsequent regulations[410] also include provisions about video surveillance.[411] The Act allows video surveillance 'of a place which is regularly frequented by a limited group of people' only if there is a special need for it.[412] Notice must be provided to surveillance subjects.[413] In addition, the Act prohibits disclosure of personal data collected by means of the surveillance without the consent of the person recorded to anyone other than the data controller or the police (in connection with the investigation of criminal acts or accidents).[414] The *Personal Data Regulations* in turn specify storage, use and erasure rules for recorded images captured from surveillance.[415] They also regulate police access to those images.[416] Finally, they guarantee individuals the right to access recordings made of them.[417]

SPECIFIC LEGISLATION ABOUT PUBLIC PLACE SURVEILLANCE

5.173 A number of countries have separate laws that specifically regulate surveillance in public places. The Swedish *Public Camera Surveillance Act* and *Public Camera Surveillance Ordinance 1998* require users of overt surveillance in public places to obtain a permit from the County Administrative Board.[418] Permits are required regardless of whether the camera images are stored.[419] Some users are exempted from the permit requirement and merely have to notify the Board about their use of surveillance.[420] Notification is sufficient to permit a post office, bank or store to use surveillance to cover entrances, exits and cash points.[421]

5.174 Installation of surveillance devices is allowed only for crime prevention and detection purposes. Cameras must be fixed and not zoomable. Moreover, an application is approved only if the user's interest outweighs the interests of the individuals subject to the surveillance, though some surveillance uses, such as uses by banks, will be always be acceptable. Finally, people who may be affected by the surveillance must be heard before any decision is made.

5.175 The fact that everyone, including the police, is required to apply to use CCTV in Sweden is a strong control measure[422] which restricts its use. In practice, however, the County Administrative Boards are unable adequately to supervise surveillance systems due to a lack of funds, and a Swedish Helsinki Committee study found many systems were in breach of the law by failing to post signs and conducting surveillance in respect of larger or different areas to those for which their surveillance systems were approved.[423]

5.176 Denmark regulates public surveillance under its *Law on the ban against TV surveillance*. The law initially applied only to private users of surveillance, prohibiting CCTV surveillance in areas open to public traffic. The law contained a number of exceptions, including for petrol stations and shopping malls.[424] Surveillance users exempted from the prohibition were still required to provide notice to the public that CCTV was used.[425]

5.177 In 1999, Denmark expanded the law to cover public authorities, requiring them to give adequate warning through signage when undertaking TV surveillance of public places.[426] In November 2004, a Danish district court found a person guilty of violating the law, for having set up webcams in a public place and broadcasting images onto the internet.[427]

5.178 France has relatively strong regulation of private users of surveillance but, somewhat controversially,[428] its surveillance regulation regime does not apply to police. A 1995 law and 1996 decree require private users of surveillance to obtain pre-approval of CCTV installation from the Prefect in their administrative region.[429] The Prefect consults with a local committee presided over by a judge. The applicant must show that the area under surveillance is particularly liable to theft or attack.

RECENT DEVELOPMENTS

5.179 Recently some countries have implemented legislation that facilitates greater surveillance practices in certain circumstances, including the use of CCTV. The trend is evident both in relation to public and private sector use of CCTV. The reasons for this legislation appear to be concerns about terrorism and other crime.

5.180 Thus, in the Netherlands, the *Camera Surveillance Act*, passed in 2005, makes it easier to use cameras for law enforcement purposes, expanding their use beyond maintenance of public order.[430] The Swedish parliament is also considering legislation to facilitate surveillance, having temporarily postponed a 2006 bill that would extend the use of secret surveillance, including telephone tapping for preventative reasons.[431] In July 2007, Denmark enacted a new law to give private companies greater rights to use CCTV, allowing them to monitor outdoor public spaces in proximity to their entrances and building fronts, whereas concerns about personal rights had previously barred private surveillance of public places such as sidewalks.[432]

5.181 Similarly, France passed an anti-terrorism law in June 2006 making it easier for private parties to install CCTV cameras in public places. The law allows cameras to be installed in areas particularly exposed to terrorist acts, violence or theft. In addition, it has expanded permitted police uses of surveillance, allowing French police to monitor cars, take photographs of number plates as well as the car's occupants, for matters ranging from terrorism to stolen vehicles.[433]

INVASION OF PRIVACY RIGHT OF ACTION

5.182 In a number of common law countries, a cause of action for invasion of privacy is available to people who suffered harm because of public place surveillance activities. In some countries, this right was established by the courts, while in others it exists because of legislation.

5.183 In the United States, four privacy torts are recognised by the courts, two of which are relevant to surveillance:

- unreasonable intrusion upon the seclusion of another
- unreasonable publicity given to an individual's private life.[434]

5.184 The tort of unreasonable intrusion requires that the intrusion be 'highly offensive to a reasonable person'.[435] This means that the interference with seclusion is a substantial one and involving conduct that a reasonable person would strongly object to.[436] A recognised example is a press photographer who enters the hospital room of a woman who has a

407 Ibid 221.

408 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 222.

409 *Act of 14 April 2000, No 31 relating to the processing of personal data (Personal Data Act)* (Norway).

410 *Regulations on the processing of personal data (Personal Data Regulations)*, by decree of 15 December 2000, Chapter 8.

411 See *Act of 14 April 2000, No 31 relating to the processing of personal data (Personal Data Act)* (Norway) Ch VI–VIII; *Regulations on the processing of personal data (Personal Data Regulations)*, by decree of 15 December 2000, Chapter 8; Carsten Wiecek and Ann Rudinow Sætnan, *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark* (2002) 15–16.

412 *Personal Data Act* [Norway] s 38.

413 *Personal Data Act* [Norway] s 40.

414 *Personal Data Act* [Norway] s 39.

415 *Personal Data Regulations* [Norway] rr 8-2, 8-4.

416 *Personal Data Regulations* [Norway] r 8-3.

417 *Personal Data Regulations* [Norway] r 8-5.

418 Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2006: An international survey of privacy laws and developments* (2007) 917; *Lag om allmän kameraövervakning*, SFS 1998:150 (Sweden) s 5 (certain users, such as banks, may merely notify the Board: ss 11–12), The act also requires clearly visible notices that surveillance is taking place (s 3), and imposes rules on the storage of any records made (s 14)

419 British Institute of International & Comparative Law, *Report: The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, Service Contract CNS/2002/AO-7002/A/55 (2003) 62.

420 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (2007) 917.

421 Ibid.

422 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 223.

423 Ibid 224.

424 Carsten Wiecek and Ann Rudinow Sætnan, *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark* (2002) 12-13.

425 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 218.

426 Carsten Wiecek and Ann Rudinow Sætnan, *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark* (2002) 13.

427 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007) 402.

428 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 222-223.

429 Ibid; British Institute of International & Comparative Law, *Report: The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, Service Contract CNS/2002/AO-7002/A/55 (2003) 20.

430 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007) 707.

431 Ibid 918.

432 Scott Berman, 'New Video Surveillance Law Fights Crime, Protects Rights', *AmCham Denmark* (Denmark), 6 June 2007, < http://www.amcham.dk/news.php?sec=news&id=303> at 28 January 2009.

433 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007) 461-462.

434 The four privacy torts were first identified by Professor William Prosser who surveyed the case law existing at the time. William Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389. The Restatements of the Law, published by the American Law Institute to give judges and lawyers greater certainty about the what the law is (see American Law Institute, *About ALI* <http://www.ali.org/index.cfm?fuseaction=about.instituteprojects> at 20 January 2009) adopted his formulation of the torts, identifying them as 1) unreasonable intrusion upon the seclusion of another; (b) appropriation of the other's name or likeness; (c) unreasonable publicity given to the other's private life; and (d) publicity that unreasonably places the other in a false light before the public. *Restatement of the Law, Second, Torts* (1977) § 652A ('General Principles').

435 *Restatement of the Law, Second, Torts* (1977) § 652B ('Intrusion Upon Seclusion').

436 *Restatement of the Law, Second, Torts* (1977) § 652B ('Intrusion Upon Seclusion'), Comment (d).

rare illness and takes her photograph, even though she previously objected to giving an interview.[437] Importantly, the intrusion itself subjects the defendant to liability, even where he or she has not published information gained from the intrusion.[438]

5.185 The tort of unreasonable publicity similarly requires that the information publicised be of a kind that is highly offensive to a reasonable person and not of legitimate concern to the public.[439] In contrast to the tort of unreasonable intrusion, however, publication is a necessary element of the tort of unreasonable publicity.

5.186 In New Zealand, a tort of invasion of privacy has also been recognised. While that tort is in the process of development, the Court of Appeal held in 2004 that it extends to wrongful publicity given to private lives.[440] The Court of Appeal of New Zealand decided in *Hosking v Runting* that the longstanding cause of action for breach of confidence was unsuitable to cover the full range of privacy concerns and that the common law should recognise a tort of invasion of privacy. [441] The elements of this new tort of privacy invasion are:

a. the existence of facts in respect of which there is a reasonable expectation of privacy
b. publicity given to those private facts that would be considered highly offensive to an objective reasonable person.[442]

5.187 In *Hosking v Runting* the NZ Court of Appeal concluded that the elements of the new tort were not made out by a celebrity couple who were seeking to prevent publication of photographs taken on a public street of their 18 month old twins. The court found both that the photographs did not publicise a fact in respect of which there was a reasonable expectation of privacy, and that their publication was not one which a person of ordinary sensibilities would find highly offensive or objectionable.[443] The court held that the photographs only disclosed that which could be seen by any member of the public in that area on the particular day, and there was no harm in publication of the ordinary photographs, notwithstanding that they were of children.[444]

5.188 As we have seen, while the common law of the United Kingdom does not yet clearly acknowledge the existence of separate tort for invasion of privacy, the action for breach of confidence is evolving into a tort concerned with the protection of privacy interests.[445] The precise nature of the interests protected by this body of law is being developed on a case by case basis.

5.189 Like the US 'publicity to private information tort' and the New Zealand privacy invasion tort, the expanded action for breach of confidence in the UK requires some wrongful use of information that is private. The following elements must be met to establish a cause of action for breach of confidence:

- information must be confidential in nature
- it must be imparted in circumstances importing an obligation of confidence
- its unauthorised use is to the detriment of the party communicating it.[446]

5.190 However, in *Douglas v Hello! Ltd*, Lord Phillips noted that the second element of the cause of action would no longer be necessary, if the information is plainly confidential. Moreover, under the expanded action for breach of confidence, one may substitute the word 'private' for the word 'confidential'.[447] Lord Phillips held that private information may be defined as 'information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public.'

5.191 In the earlier case of *Campbell v MGM*, Lord Hope noted that while in some cases, the answer to the question what is private information will be obvious, where it is not, 'the broad test is whether disclosure of the information about the individual (A) would give substantial offence to A, assuming that A was placed in similar circumstances and was a person of ordinary sensibilities'.[448] This is the same test as in the Australian case, *Lenah Game Meats*.

5.192 However, Lord Hope reminds us that this the 'highly offensive test' only applies in cases where there is room for doubt; it is not to be used where information can easily be identified as private:[449]

> *if the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected. So there is normally no need to go on and ask whether it would be highly offensive for it to be published.*[450]

5.193 This view was shared more recently by the Court of Appeal in *Murray v Big Pictures (UK) Ltd*, where the court said that the 'highly offensive test' is not used for determining whether privacy has been breached, but whether the breach of privacy is not outweighed by countervailing considerations such as freedom of expression.[451] *Murray* concerned a photograph taken covertly on a public street of the famous author J.K. Rowling and her family. The court distinguished the UK expanded breach of confidence test from the invasion of privacy tort in New Zealand, where the 'highly offensive test' is part of making an initial case for a breach of privacy.[452]

STATUTORY CAUSES OF ACTION FOR INVASION OF PRIVACY

5.194 Some parts of Canada and the United States have passed legislation which creates a cause of action for invasion of privacy.[453] For example, legislation in Canadian provinces generally provides that 'it is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person.'[454] The legislation stipulates a number of general defences, and provides a number of remedies, including damages.[455]

5.195 The law reform commissions of two other common law countries have recommended a statutory cause of action for an invasion of privacy. For example, the Hong Kong Law Reform Commission has recommended the creation of two statutory torts to protect individuals from unreasonable invasion of privacy:

1) unwarranted intrusion upon the solitude or seclusion of another
2) unwarranted publicity concerning an individual's private life.[456]

The Hong Kong Commission observed that 'an individual's right to privacy does not automatically cease when he leaves the confines of his home or other secluded premises' and that 'a person can be visible to the public without forfeiting his right to the privacy of his communications'.[457] On the other hand, the Commission suggested that a person does not normally have a reasonable expectation of privacy from visual surveillance when in an area visible to the public.[458]

5.196 The Law Reform Commission of Ireland has recommended the enactment of a 'civil tort directed against acts of privacy-invasive surveillance in circumstances where a "reasonable expectation" of privacy exists'.[459] The Commission acknowledged that there was a reduced expectation of privacy in public places, commenting that 'the taking of casual photographs in a public place should not normally be held to be an invasion of the privacy'. It suggested, however, that 'the targeting of a particular individual either surreptitiously or against his or her will in a public place, *particularly with a view to publication of that person's photograph*, could well, depending on the circumstances, be held to be an invasion of that person's privacy'.[460]

437 *Restatement of the Law, Second, Torts* (1977) § 652B ('Intrusion Upon Seclusion'), Illustration 1.

438 *Restatement of the Law, Second, Torts* (1977) § 652B ('Intrusion Upon Seclusion'), Comment (b).

439 *Restatement of the Law, Second, Torts* (1977) § 652D ('Publicity Given to Private Life').

440 *Hosking v Runting* [2003] 3 NZLR 285, [117].

441 *Hosking v Runting* [2003] 3 NZLR 285, which has made it very difficult for plaintiffs to bring privacy suits against media organisations.

442 *Hosking v Runting* [2003] 3 NZLR 285, [117].

443 *Hosking v Runting* [2003] 3 NZLR 285, [164]–[165].

444 *Hosking v Runting* [2003] 3 NZLR 285, [164]–[165].

445 *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB) [7] (Eady J).

446 *Coco v AN Clark (Engineers) Ltd* [1968] FSR 415, 419 (Megarry J).

447 *Douglas v Hello! Ltd* [2005] EWCA Civ 595, [83], [118].

448 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457, [92].

449 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457, [94].

450 *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457, [96].

451 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, [26].

452 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, [48]–[49].

453 See generally Fred H Cate, *Privacy in the Information Age* (1997) 88; John D R Craig, Invasion of Privacy and Charter Values: The Common-Law Tort Awakens (1997) 42 *McGill Law Journal* 355, 362.

454 *Privacy Act 1978* RSS c P-24 (Saskatchewan) s 2; see also *Privacy Act 1996* RSBC c 373 (British Columbia) s 1(1); *Privacy Act* CCSM s P125 (Manitoba) ss 2(1)–2(2); *Privacy Act 1990* RSNL c P-22 (Newfoundland and Labrador) s 3(1).

455 *Privacy Act 1978* RSS c P-24 (Saskatchewan) ss 4, 7; *Privacy Act 1996* RSBC c 373 (British Columbia) s 2; *Privacy Act* CCSM s P125 (Manitoba) ss 4(1), 5; *Privacy Act 1990* RSNL c P-22 (Newfoundland and Labrador) ss 5, 6(1).

456 Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* Report (2004) 277–9, [13.1]–[13.14].

457 Ibid 127, [6.51].

458 Ibid 128, [6.55].

459 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998) [1.5]. A privacy bill which would largely implement the Law Reform Commission's recommendations was introduced into the Irish Parliament in 2006. If enacted, it will create a new right of action for invasion of privacy. As at January 2009, the Bill had not been enacted. The bill is available at <www.oireachtas.ie/documents/bills28/bills/2006/4406/b4406s.pdf>.

460 Ibid [2.13] (emphasis in original). A privacy bill, which would have largely implemented the Law Reform Commission's recommendations, was introduced into the Irish Parliament in 2006. If enacted, it would create a new right of action for invasion of privacy. As at January 2009, the Bill had not been enacted. See The Privacy Bill 2006 (Ireland) <http://www.oireachtas.ie/documents/bills28/bills/2006/4406/b4406s.pdf> at 29 January 2009.

Current Law

5.197 As discussed above, the ALRC has recommended the introduction of a statutory cause of action for invasion of privacy,[461] modelled on a recommendation made by the NSWLRC in 2007.[462] The cause of action includes a non-exhaustive list of the circumstances that could give rise to the cause of action.[463] The ALRC suggests that one of those circumstances would be being subjected to 'unauthorised surveillance'.[464]

CONCLUSION

5.198 While the practice of surveillance in public places continues to grow in Victoria, the law has not kept pace with the expanded capabilities and uses of surveillance devices. These devices have become increasingly affordable, available and sophisticated. The two major bodies of law regulating public place surveillance— the SDA (Vic) and information privacy laws—have major limitations in their application to public place surveillance, because they were not specifically designed to regulate this activity.

5.199 The development of laws to cover particularly offensive forms of surveillance, such as upskirting and surveillance related to child pornography, and to regulate some industries, for example casinos and bars, has been an attempt to address some of the limitations in the current regime. The result has been piecemeal regulation. We do not have laws of general application, based on a set of guiding principles, that seek to balance the competing interests at stake when surveillance devices are used in public places. In the next chapter we describe a number of reform options that may fulfil this role.

461 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108 (2008) 88 (Recommendation 74–1).

462 NSW Law Reform Commission, Invasion of Privacy, Consultation Paper 1 (2007).

463 Ibid 158; Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108 (2008) 88 (Recommendation 74–1).

464 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108 (2008) 88 (Recommendation 74–1).

Chapter 5 Current Law

TABLE 1: LEGISLATION AND BINDING CODES RELATING TO PUBLIC PLACE SURVEILLANCE IN VICTORIA

LEGISLATION	APPLICATION TO PUBLIC PLACE SURVEILLANCE	USERS COVERED
Privacy Act 1988 (Cth).	Regulates the collection, use, storage and disclosure of 'personal information' about individuals, including surveillance captured information that is recorded and in which a person is potentially identifiable.	Commonwealth government agencies and large businesses.[465]
Surveillance Devices Act 2004 (Cth).	Establishes procedures for law enforcement officers to obtain warrants for the installation and use of surveillance devices in relation to the investigation of certain offences; regulates the use and disclosure of information collected.	Commonwealth and state law enforcement officers.
Telecommunications (Interception and Access) Act 1979 (Cth).	Prohibits interception of telecommunications systems and access to stored communications without a warrant in most circumstances. Establishes procedures for the issuing of warrants for national security and law enforcement activities.	All
Casino Control Act 1991 (Vic) ss 59(2), 122(1)(r).	Gives the Victorian Commission for Gambling Regulation control over the operation of security cameras at gaming venues in Victoria and requires that it develop procedures for their use.	Gaming venues.
Charter of Human Rights and Responsibilities Act 2006 (Vic) ss 7, 13.	Makes it unlawful for public authorities to act in a way that is incompatible with human rights listed in the Charter, including the right not to have privacy arbitrarily interfered with. Requires any interference (such as through surveillance, recorded or unrecorded) to be demonstrably justified.[466]	Victorian government agencies and contracted service providers.
Crimes Act 1958 (Vic) s 68.	Prohibits the production of child pornography.	All
Crimes Act 1958 (Vic) s 21A.	Prohibits stalking.	All
Information Privacy Act 2000 (Vic).	Regulates the collection, use and disclosure of 'personal information' (other than health information) about individuals, including surveillance captured information that is recorded and in which a person is potentially identifiable.	Victorian government agencies and contracted service providers.

Surveillance Devices Act 1999 (Vic).	Prohibits, in different circumstances, listening and optical surveillance devices to monitor private conversations and activities, and the use of tracking devices. Establishes exceptions, for example for authorised law enforcement activities. Prohibits the use of data surveillance devices by law enforcement officers in most circumstances unless a warrant is obtained.	Everyone, other than Australian Federal Police and some other Commonwealth agencies.
Liquor Control Reform Act 1998 (Vic) s 18B	Provides that installation of security cameras may be a condition for a liquor licence, and standards on their quality and operation may apply.	Liquor venues.
Summary Offences Act 1966 (Vic) div 4A.	Prohibits upskirting.	All
Summary Offences Act 1966 (Vic) s17	Prohibits indecent, offensive or insulting behaviour in public	All
Private Security Act 2004 (Vic) s 25 (3).	Provides that a requirement of being granted a private security licence is the successful completion of training in relation to each activity for which the licence is granted (including private investigation).	Private security individuals and businesses.
Transport (Taxi-Cabs) Regulations 2005 (Vic) s 15, 22	Requires that taxis be fitted with surveillance cameras and that the installation be approved by a regulator. Prohibits interference with the cameras.	Taxi operators and drivers.
Transport Act 1983 (Vic) s 144.	Makes it a condition of a taxi licence that equipment capable of transmitting images from a surveillance camera or making an audio recording must not be installed in a taxi.	Taxi operators and drivers.
BINDING CODES	**APPLICATION TO PUBLIC PLACE SURVEILLANCE**	**USERS COVERED**
Biometrics Institute Privacy Code (Cth)	Substantially similar to the NPPs, however tailored to organisations using or planning to use biometrics.	Biometrics Institute members who have agreed to be covered by the Code.
Market and Social Research Privacy Code (Cth)	Substantially similar to the NPPs, however tailored to the market and social research context.	Association of Market and Social Research Organisations members.
Media codes[467]	Not necessarily substantially similar to the NPPs. Generally require a public interest justification to breach the right to privacy with respect to private matters in public places. Similarly, require public interest justification for covert surveillance.	Signatory media organisations.

465 'Large businesses' are defined as businesses with an annual turnover of over $3 million. Privacy Act 1988 (Cth) s 6D(1)-(2). Media organisations may be exempted.

466 Individuals cannot take action under the Charter unless they have an existing basis, or cause of action, for challenging the unlawful activity: Charter of Human Rights and Responsibilities Act 2006 (Vic) s 39(1).

467 See, eg, Australian Communications and Media Authority, Privacy Guidelines for Broadcasters (2005) and Privacy Standards, Australian Press Council

Current Law

TABLE 2: MAJOR NON-BINDING INSTRUMENTS RELATING TO PUBLIC PLACE SURVEILLANCE IN VICTORIA

GUIDELINES			
Organisation	**Instrument**	**Application to public place surveillance**	**Users covered**
Victorian Privacy Commissioner	Guidelines relating to information privacy laws[468]	Guidance on how to comply with various aspects of information privacy laws.	Victorian government agencies and contracted service providers.
Victorian Privacy Commissioner	Information sheets on various aspects of surveillance.[469]	Discussion of the privacy implications of types of surveillance devices, and policy measures to prevent their abuse.	Relevant surveillance users.
Federal Privacy Commissioner	*Covert Surveillance in Commonwealth Administration: Guidelines*	Guidance on agencies' responsibilities in carrying out covert surveillance activities.	Commonwealth government agencies.
Department of Infrastructure (Vic)	*Policy and Procedures for the Management of CCTV Evidence Records*	Establishes a system for the handling of CCTV footage, including that it be treated in accordance with privacy principles contained in the *Information Privacy Act 2000* (Vic).	Public transport systems.
Australian Institute of Petroleum	*Guidelines for Service Station Security*	Provides guidance to petrol station owners and staff relating to their responsibilities in carrying out surveillance.	Petrol stations owners and staff.
VOLUNTARY STANDARDS			
Organisation	**Instrument**	**Application to public place surveillance**	**Users covered**
Australian Retailers Association	*Radio Frequency Identification (RFID) in Retail: Consumer Privacy Code of Practice*.	Designed to protect consumer privacy; covers areas including notice to consumers, education, and retention, use and security of data.	Retail outlets.

Council of Australian Governments (COAG)	*National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism*	Standards for use of CCTV systems on mass passenger transport. Covers permissible uses and disclosure of surveillance footage for counter-terrorism purposes and recommends community consultation on camera location and installation.	Specified forms of mass public transport, including trains, trams and buses.
Department of Justice (Vic)	*CCTV Toolkit for Victoria*	Recommendations for evaluating the usefulness of a proposed CCTV system. Includes the recommendation that users consult with community groups to ensure privacy is respected.	All
Standards Australia	*Australian Standard: Closed circuit television (CCTV), Parts 1–3*	Include recommendations on the operation, management, selection, planning and installation of CCTV systems. Outlines good practice, including that cameras not be used to infringe the individual's privacy rights.	All
Individual businesses	Internal policies	Policies on placement of cameras and 'no-go' areas for cameras, signage, access to footage by staff, inappropriate use of surveillance cameras, disclosure to third parties, etc.	Government and private sector users.

468 See, eg, Office of the Victorian Privacy Commissioner, Who's covered by the Information Privacy Act?, Info Sheet 01.06 (2006); Office of the Victorian Privacy Commissioner, Short Guide to the Information Privacy Principles (2006); Office of the Victorian Privacy Commissioner, Model Terms for Transborder Data Flows of Personal Information, Guidelines Edition.01 (2006).

469 See, eg, Office of the Victorian Privacy Commissioner, Mobile Phones with Cameras, Info Sheet 5.03 (2003), Office of the Victorian Privacy Commissioner, Privacy and Global Positioning System Technology, Info Sheet 2.08 (2008), Office of the Victorian Privacy Commissioner, Images and privacy, Info Sheet 1.03 (2003).

Chapter 5 Current Law

Chapter 6

Options for Reform

Chapter 6 Options for Reform

INTRODUCTION

6.1 It is time to reconsider the regulatory framework that governs surveillance in public places in Victoria because of the widespread use of surveillance and the increasing sophistication of surveillance technology. In this chapter we present a number of options for reform designed to provide more comprehensive regulation of public place surveillance than exists under our current laws. We aim to stimulate public discussion and debate about this issue to assist us in developing recommendations for change that will be included in our final report to the Attorney-General.

6.2 Devising a regulatory framework for surveillance in public places is a complex undertaking. Different forms of surveillance are used in Victorian public places for varying purposes. In view of these differences, the commission believes that a multifaceted response to the increased use of surveillance in public places is appropriate. We have devised a number of reform options that range from a monitoring role for a regulator, to requiring people to obtain a licence to use some devices that have the capacity to be particularly invasive of privacy, to a new legally enforceable obligation upon everyone to refrain from gross invasions of people's privacy. The commission does not have a final view about any of these options.

THE CASE FOR REFORM

6.3 It is clear that surveillance in public places has become more widespread. Its use is increasing as technology becomes more sophisticated and affordable.[1] A number of writers have commented on the possible impact of public place surveillance.[2] They include Benjamin J Goold who has identified some of the fundamental issues that require consideration when determining how we should regulate the use of surveillance in public places:

> *while most of us accept that we surrender a certain amount of personal privacy once we leave the confines of our own home, few would concede that we have no expectation of privacy when we stand on the street or walk through a park. The problem lies with identifying the interests that are harmed by the absence of privacy protections in such circumstances. How, for example, is being watched by a CCTV camera different from being watched by a stranger sitting on a park bench or, for that matter, by a police officer standing on a street corner?*
>
> *Put simply, does the fact that we appear to have little or no control over the rest of the world in public mean that we surrender any expectation of privacy when we step out onto the street or go for a walk in a park?*[3]

6.4 People do not surrender all expectations of privacy when they enter public places. Most of us have zones of intimacy involving parts of our body and bodily processes that we want to keep private. We expect others to observe our right to do so at all times, even when in public. We also have expectations of privacy about aspects of our image, communications and movements, even when in public. Our expectations of privacy will often depend on the circumstances, such as whether any surveillance activity is noticeable.

6.5 Being watched by a CCTV camera in a public place is very different to being watched by a stranger, or even a police officer, on the street because of the issue of awareness. Most people have the capacity to notice the presence of a stranger, to assess that stranger's ability to observe them or overhear their conversations and to moderate their behaviour accordingly. By contrast, people will often not be aware of the existence of a CCTV camera, or of its capacity to observe aspects of their image or their communications.

6.6 As Goold notes, before considering the nature of any regulatory response to the use of surveillance in public places, it is necessary to consider what harm may result if individual expectations of privacy in public places are threatened by the uncontrolled use of surveillance devices.[4] That harm may be both subtle and incremental.[5] Daniel Solove has suggested that some invasions of privacy are similar to cumulative environmental harms or pollution because of the long-term 'chilling effect'[6] they may have upon individual and

collective behaviour.[7] A further challenge when contemplating regulation of surveillance is that 'in many instances, there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value.'[8]

6.7 Commentators suggest that surveillance threatens anonymity. Andrew Von Hirsch, for example, has written about interferences with our 'anonymity conventions' through the possibility of prolonged scrutiny from unobservable observers.[9] It is argued that the loss of privacy and anonymity in public places threatens cherished freedoms, such as freedom of communication and movement, and widely shared human values, such as individual and communal senses of dignity and autonomy.

6.8 As the use of surveillance cameras becomes more widespread, deeply felt apprehension about unknown and unseen monitoring of our activities in public places may alter the way in which we function as a community. We may lose the capacity to behave and communicate with any sense of freedom outside the confines of our private spaces. Public places may come to be regarded as 'observed places'.

6.9 Goold describes the harm which may flow from the unregulated use of CCTV:

> *One does not have to be suffering from any deep-seated Orwellian paranoia to recognize that the establishment of a widespread network of surveillance cameras may have serious implications for civil liberties and the exercise of state power…As the experience of the United Kingdom has shown, there is a very real danger that once a certain momentum has been achieved the spread of CCTV systems will be hard to arrest…*[10]
>
> *Under the gaze of CCTV, it is simply impossible to blend into the situational landscape, or to be confident that one is acting anonymously. Looked at in this way, the argument that those who have nothing to hide have nothing to fear has little purchase. Even if I am not committing an illegal act or behaving in a way that might be expected to draw the attention of those behind the cameras, the mere fact that I am being watched and my activities possibly recorded may be enough to make me 'second guess' my own behavior – and therefore diminishes the sense of freedom and autonomy that comes from being in public.*[11]

6.10 The nature of much of the potential harm caused by the abuse of surveillance and the inability of individuals to be aware of particular instances of abuse means that only government can effectively regulate surveillance in public places. If surveillance, like environmental pollution, has the potential to threaten the entire community if not properly regulated, governments must devise and implement appropriate controls. The legitimate interest that public authorities and private organisations have in using surveillance devices to safeguard against threats to public safety and interference with property must be balanced against the potential damage to individual and community interests. Government is best placed to balance these competing interests and to discourage or prevent the inappropriate use of surveillance.

OUR PROCESS FOR DEVELOPING OPTIONS FOR REFORM

6.11 We have undertaken the following process in order to develop reform options:

- Firstly, we have assessed the existing regulatory framework for surveillance in public places in Victoria. Our options aim to address its shortcomings.
- Secondly, we have considered regulatory practices in other jurisdictions (both interstate and overseas) that might serve as models for improved regulation of public place surveillance in Victoria. We have also examined Australian approaches to regulation in other rapidly changing areas of public concern, such as the environment. In addition, we have reviewed the recommendations by other reform bodies that are relevant to surveillance in public places. In particular, we have considered the recommendations by the Australian Law Reform Commission (ALRC) concerning reform of information privacy laws.[12]

1 Current surveillance practices are discussed in Chapter 2.

2 We discuss the risks and benefits of public place surveillance in Chapter 4.

3 Benjamin Goold, 'Privacy Rights and Public Spaces: CCTV and the Problem of the "Unobservable Observer"' (2002) 21 (1) *Criminal Justice Ethics* 21, 21–2.

4 Benjamin Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance"' (2006) 25 (1) *Criminal Justice Ethics* 3, 5.

5 This is discussed further in Chapter 4.

6 A 'chilling effect' is the tendency to avoid engaging in speech or conduct knowing that to do so will have undesirable consequences. For an example of the chilling effect in US constitutional law see: *Lamont v Postmaster General*, 381 US 301 (1965).

7 Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477, 488.

8 Ibid 563.

9 Andrew von Hirsch, 'The Ethics of Public Television Surveillance ' in Andrew von Hirsch, et al (eds) *Ethical and Social Perspectives on Situational Crime Prevention* (2000) 59, 64-65.

10 Benjamin Goold, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance"' (2006) 25 (1) *Criminal Justice Ethics* 3, 4.

11 Ibid 6.

12 Chapter 5 considers all of these issues in detail.

Chapter 6 Options for Reform

- Thirdly, we have considered the initial views expressed in our preliminary consultations with surveillance users, advocates and community groups about the desired form of any future regulation. We summarise these views below.
- Fourthly, we have looked at what constitutes effective regulation in any context. Where possible, we have attempted to ensure that our options for reform meet the standards for good regulation proposed by regulatory theorists and embodied in other regulatory models. We discuss some of this literature in brief, below.
- Finally, we have developed a set of overarching draft principles that may be used to guide any regulatory changes and inform policy in relation to public place surveillance in Victoria. These principles, which draw upon relevant rights enshrined in the Victorian Charter of Human Rights, are similar to principles developed elsewhere to guide surveillance practice.

SUMMARY OF GAPS IN THE CURRENT REGULATORY FRAMEWORK

6.12 No single body of law comprehensively regulates the use of surveillance in public places in Victoria. There is legislation that regulates the use of some surveillance devices in limited circumstances and laws which restrict the capacity of some organisations to gather and use private information acquired by any means.[13] There is, however, no clear public policy concerning the circumstances in which public place surveillance is acceptable and those circumstances in which it is not permissible.

6.13 The three main Acts that regulate surveillance in public places in Victoria are the *Surveillance Devices Act 1999* (Vic) (SDA), the *Privacy Act* (Cth) and the *Information Privacy Act 2000* (Vic) (IPA).

6.14 The policy which underpins the SDA (Vic) is not clear and it has been overtaken by technological developments. For reasons which are not readily apparent, the Act regulates the use of different devices in different ways. The Act does not deal with what is known as device convergence, which makes distinctions between different categories of devices increasingly irrelevant. For example, a mobile phone can now record images and track an owner's movements. The enforcement regime in the SDA (Vic) is not very sophisticated. The SDA (Vic) is one of the many statutes which create criminal offences that fall under the general supervision of Victoria Police.[14] No regulator has specific responsibility for ensuring that members of the community are aware of the Act and comply with it. Indeed, there does not appear to be widespread community awareness of the legislation. We are not aware of any prosecutions under the Act.

6.15 The Privacy Act (Cth) and the IPA (Vic) contain privacy principles concerning the collection of 'personal information', and the use, disclosure, retention and disposal of that information. These laws apply to some uses of surveillance in public places. Many acts of surveillance may not be subject to information privacy laws because the material collected does not fall within the definition of 'personal information'. Personal information is defined as recorded information about an individual whose identity is apparent, or may reasonably be ascertained, from that information.[15] In addition, information privacy laws do not apply to all users of surveillance. Notable exemptions are individual users of surveillance,[16] and businesses with an annual turnover of $3 million dollars or less.[17]

6.16 A central issue that arises under the current regulatory framework is consent to the activity in question. Both the SDA and information privacy laws do not apply when a person has consented to surveillance activity. That consent may be express or implied. The circumstances in which consent may be implied are sometimes unclear. For example, the notion of consent may be illusory if a person has no alternative means of accessing a place or service other than by 'consenting' to surveillance activity.

Surveillance is also regulated by a range of industry and government codes, self-imposed policies, standards and guidelines. The effect of this type of voluntary regulation is limited because of its voluntary nature and because there is no external oversight of compliance with the requirements of voluntary guidelines. There do not appear to be any government-wide policies that govern the use and funding of surveillance activities by public agencies.

6.17 The existing Victorian regulatory regime is not well equipped to deal with the challenges posed by current and emerging surveillance technology. The gaps in the existing regulatory framework (discussed in Chapter 5) are significant. Some of the relevant laws have been overtaken by developments in technology and others were not designed to deal with surveillance activities. These deficiencies mean that it is time to consider reform proposals.

INITIAL VIEWS EXPRESSED TO THE COMMISSION

6.18 During 2006 and 2007 we conducted 31 roundtable discussions with various groups in Victoria representing both users of public place surveillance and individuals likely to be the subject of surveillance. The groups included state government organisations, police, local councils, universities and TAFE institutions, transport operators, businesses (including media organisations, retailers and sports and entertainment venues), courts, security and investigation organisations, indigenous justice bodies, young people, and other community representatives and private citizens.

6.19 We asked those we consulted whether regulation of public place surveillance can be improved in Victoria, and if so how. A summary of their views expressed at the time follows.

No outright prohibition

6.20 A number of groups warned against an outright prohibition of surveillance in public places. For example, in roundtables with sporting and entertainment venues putting controls on surveillance camera use, rather than prohibition, was favoured.[18] Police warned that prohibiting surveillance in certain areas led to offenders gravitating to those areas thereby making them unsafe.[19]

6.21 Community groups told the commission that regulation should distinguish between innocent and problematic uses of surveillance, and that it should not restrict common activities such as the taking of holiday photographs.[20]

Guidelines and codes

6.22 Many surveillance users supported the idea of standards to guide practice.[21] They told us that 'guidelines' are important and that other jurisdictions have used them successfully.[22] Media groups noted that having simple, easy to understand information on what they can and cannot do, would be useful.[23] Sporting and entertainment venues favoured 'codes of practice' and 'guidelines' to complement existing law.[24]

6.23 Some individuals subject to surveillance favoured stronger protections than voluntary guidelines or codes. In one of our roundtables with community organisations it was emphasised that law reform should not lead to an erosion of current protections.[25] Some called for greater legislative protection and argued that privacy law would develop at an unacceptably slow pace in the courts.[26] Similarly, some young people expressed the view that mere protocols were not enough and that there needs to be recourse of a legal nature.[27]

Other forms of regulation favoured

6.24 The police favoured the registration of CCTV systems, as this would assist them in knowing the location of these systems.[28] In addition, some groups favoured the use of licences for surveillance systems.[29]

6.25 Public education was also favoured. In a community roundtable that included youth, homeless and human rights organisations, it was suggested that there should be a public education campaign about surveillance.[30] It was also suggested that there is a need to raise public awareness about the use of surveillance.[31]

13 The current regulatory framework for surveillance in public places in Victoria is discussed in Chapter 5.

14 Because the SDA (Vic) contains criminal offences, Victoria Police has a general responsibility to act in response to suspected or reported breaches of that Act.

15 This concept is discussed in detail in Chapter 5.

16 *Privacy Act 1988* (Cth) s 16E.

17 However, the commission notes that the ALRC's recent recommendations for the removal of this exemption may bring more private businesses that use surveillance under the ambit of the *Privacy Act 1988* (Cth).

18 Roundtable 4.

19 Roundtable 5.

20 Roundtable 17.

21 Including tertiary institutions, transport groups, police, the media, sporting and entertainment venues, and some in the retail sector: Roundtables 4, 9, 14, 15, 19, 20, 23, 26.

22 Roundtable 16.

23 Roundtable 26.

24 Roundtable 4.

25 Roundtable 18.

26 Roundtable 17.

27 Roundtable 22.

28 Roundtable 30.

29 Roundtable 4.

30 Roundtable 16.

31 Roundtables 16, 18.

Chapter 6 Options for Reform

6.26 Other views expressed to the commission focussed on technology or design. For example, representatives of the Indigenous community expressed the view that cameras should have minimum technical standards to ensure that captured images are of high quality.[32]

Regulation of individual users

6.27 A few groups stressed that regulation should cover personal use of surveillance.[33] For example, it was suggested that the use of mobile phones and MP3 equipment to record individuals should be regulated.[34] In one of the community roundtables, a participant queried whether the law can appropriately regulate citizen surveillance and expressed concern about government encouraging private citizens to take up surveillance through 'dobbing' phone lines.[35]

6.28 By contrast, in a media roundtable, the commission was told that governments at all levels are already making it more difficult for commercial photography to take place in public places.[36] Reference was made to proposed restrictions on taking photographs of children on the beach.[37] A police group warned against regulating surveillance that involved personal observation without the use of a surveillance device, noting that it would not be possible to regulate people merely following each other.[38]

Extent of regulation

6.29 Many users of surveillance warned against excessive regulation. For example, in our consultation with banks, it was suggested that regulation should not hamper the efficiencies that new surveillance technologies generate, and that government should consider the economic impact on business that would flow from restricting the use of surveillance technologies.[39] Sporting and entertainment venues did not want to see regulation that was overly prescriptive, citing the *Occupational Health and Safety Act 2004* (Cth) (OHS Act (Cth)) as an example of overly prescriptive regulation.[40] Retail groups also expressed concern about over-regulation.[41]

6.30 The police suggested that unnecessary restrictions on the publication of images provided by witnesses would have a significant negative impact on criminal investigations.[42] They gave the example of police use of surveillance material on the Crime Stoppers program. That program collects information about crime, including surveillance footage, from business and individuals. The footage is included on a website in the hope of eliciting information about crime from the public. The police were also opposed to regulation that would require lengthy applications for warrants.[43]

6.31 In one of our media roundtables, the commission was warned about overly broad laws.[44] For particular problems, such as upskirting, specific legislation was considered more appropriate than widening the ambit of the law in a way that may extend to unproblematic uses of surveillance.[45] The commission was advised that the existing legal framework is a minefield for the media. It was suggested that legal advice is constantly needed on what the media can and cannot do with respect to their reporting to stay within existing laws (for example privacy and sedition laws) and that overregulation is making reporting difficult.[46]

6.32 A number of groups suggested that they ought to be eligible for some form of exemption from certain aspects of surveillance regulation. In our roundtables with police and media, a public interest exemption was raised.[47] Transport groups suggested that regulation should apply only where surveillance is undertaken 'without lawful excuse'[48] or 'for an unlawful purpose'.[49]

ELEMENTS OF EFFECTIVE REGULATION

6.33 In developing options for reform, we have also considered general principles of effective regulation. A compliance-orientated approach to regulation has much support. It focuses on persuasive and collaborative strategies to achieve cooperation with existing law.[50] The 'enforcement pyramid', developed by Professors Ian Ayres and John Braithwaite, acknowledges the importance of the compliance-oriented approach by prioritising it above more punitive approaches.[51] Under this model, regulators move progressively up the pyramid, using coercive sanctions only when less interventionist measures, such as

education, fail to produce the desired outcomes.[52] Intermediate sanctions may include warning letters and civil penalties.[53] Ultimate sanctions may include criminal penalties or loss of licence.[54] An important outcome of the model is that most of the regulatory action will occur at the base of the pyramid.[55]

6.34 The ALRC strongly supported the enforcement pyramid approach to regulating the Privacy Act in its 2008 Privacy Report,[56] and made several recommendations to widen the current range of enforcement strategies available to the Federal Privacy Commissioner, including the use of civil penalties and enforceable undertakings.[57]

6.35 We relied on an enforcement pyramid approach when we developed our workplace privacy regulatory framework.[58] Under the scheme proposed in our final report, we suggested that a regulator promote workplace privacy by encouraging voluntary compliance with the scheme.[59] In addition, we proposed that the regulator be given the power to resolve complaints informally, to conciliate complaints in appropriate cases and to make rulings which could be enforced by registration at the Victorian Civil and Administrative Tribunal (VCAT).[60] Only when those mechanisms failed did we suggest that stronger sanctions could apply.[61]

6.36 It is our preliminary view that regulation of public place surveillance should be flexible and multifaceted. It should provide sufficient flexibility to address the many contexts in which surveillance occurs and the broad range of people who use surveillance. Different rules may apply to different users of surveillance and to the same user when using different forms of surveillance. [62]

6.37 The need for regulation may also differ by context. For example, what is necessary to regulate systematic surveillance by government bodies of personal communications may be far more than what is necessary to regulate an individual engaged in random photography. When devising regulation it may be relevant to consider:

- the nature of a surveillance practice
- who is conducting the surveillance practice
- why the surveillance practice is being conducted.

PRINCIPLES TO GUIDE PUBLIC PLACE SURVEILLANCE

6.38 The commission has devised four draft policy principles that may be used to inform and guide any changes to the way in which surveillance in public places is regulated in Victoria.

6.39 We have drawn upon the principles devised by the New South Wales Law Reform Commission (NSWLRC) in its surveillance reference[63] and those developed by the ALRC in its recent report on privacy law and practice.[64]

6.40 The ALRC noted that 'principles-based regulation seeks to provide an overarching framework that guides and assists regulated entities to develop an appreciation of the core goals of the regulatory scheme'.[65] Information privacy principles and national privacy principles under the Privacy Act (Cth) regulate the collection and handling of personal information. They require, amongst other things, that organisations only collect information for a lawful purpose directly related to a function of activity of the organisation, and that they collect it by lawful and fair means.[66]

32 Roundtable 28.
33 Roundtables 9, 10, 18.
34 Roundtable 9.
35 Roundtable 18.
36 Roundtable 26.
37 Roundtable 26; see also Andrew Clark, 'These Photos May be Illegal', *The Sydney Morning Herald* (Sydney), 16 November 2005, 15.
38 Roundtable 30.
39 Roundtable 29.
40 Roundtable 4.
41 Roundtables 14, 15, 20.
42 Roundtable 5.
43 Roundtable 8.
44 Roundtable 27.
45 Roundtable 26.
46 Roundtable 27.
47 Roundtables 5 and 26.
48 Roundtable 19.
49 Roundtable 23.
50 Christine Parker, 'Reinventing Regulation within the Corporation: Compliance-Orientated Regulatory Innovation' (2000) 32 (5) *Administration and Society* 533.
51 Ibid 541.
52 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992) 35–6.
53 Ibid 35–6.
54 Ibid 35–6.
55 Ibid 35.
56 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [4.71].
57 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 2: Final Report* 108 (2008) Recs 50-2, 50-4. An enforceable undertaking is a promise enforceable in court by one who has breached the law to comply thereafter. See[50.53]–[50.55].
58 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [4.79].
59 Ibid.
60 Ibid.
61 Ibid [4.80].
62 As noted in Department of Treasury and Finance, *Victorian Guide to Regulation incorporating: Guidelines made under the 'Subordinate Legislation Act 1994' and Guidelines for the Measurement of Changes in Administrative Burden* (2nd ed, 2007) [3-1], 'excessive or poorly developed regulation can impose costs on society that outweigh the benefits of this regulation'.
63 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [4.40].
64 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [4.7].
65 Ibid.
66 See *Privacy Act 1988* (Cth) s 14 and sch 3.

Chapter 6 Options for Reform

6.41 The NSWLRC identified the following principles in relation to overt surveillance and noted that they would 'introduce clarity and consistency to the practice' of surveillance which would serve the public interest 'without imposing a burden on surveillance users.'[67]

- overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy
- overt surveillance must only be undertaken for an acceptable purpose
- overt surveillance must be conducted in a manner which is appropriate for that purpose
- notice provisions shall identify the surveillance user
- surveillance users are accountable for their surveillance devices and the consequences of their use.[68]

6.42 The European Human Rights Convention has been interpreted to require proportionality between the surveillance practice and the purpose it seeks to achieve.[69] A study into the social and political impacts of CCTV in European cities recommends allowing video surveillance in public places only for a limited set of clearly defined purposes, and making surveillance transparent.[70]

6.43 The commission acknowledges that devising overarching statements of public policy for surveillance in public places is very difficult because of the wide variety of users and contexts in which surveillance is used. Our definition of surveillance in Chapter 1 incorporates both one-off and systematic practices. The differences between these practices pose considerable regulatory challenges. For example, what the community would consider acceptable conduct by organisations and businesses who conduct surveillance on a continuous basis may differ to what would be expected from people who only intermittently use surveillance devices for example, recording footage on a mobile phone. We have attempted to reflect these differences in the draft principles.

6.44 The commission believes that overarching principles are important because they are an attempt to identify clearly the public policy upon which the law is based. It is necessary to explain and debate that policy before moving to its implementation by way of changes to the law. The commission has not reached a final view about the draft principles detailed below and is keen to receive submissions about whether they are appropriate and how they may be improved.

1. People are entitled to some privacy when in public places

6.45 The content and reasonableness of a person's expectation of privacy in public will differ according to a number of factors, including:

- the location
- the nature of the activity that is observed
- whether the activity is recorded and disseminated
- the type of surveillance used
- the identity of any particular person observed (eg a public official)
- whether the surveillance unfairly focused on a particular person or was harassing in nature
- whether the surveillance was covert
- whether the person consented to the surveillance.[71]

6.46 In 2008, the British Columbia Law Institute in Canada recommended that the Privacy Act of British Columbia be amended to include a similar principle.[72] It was suggested that the Act would state that a person 'may have a reasonable degree of privacy with respect to lawful activities of that person that occur in a public setting, and which are not directed at attracting publicity or the attention of others.'

2. Wherever practicable public place surveillance should be transparent

6.47 Transparency reduces the potential for harm by allowing people to adjust their behaviour. It also promotes accountability by subjecting surveillance practices to public scrutiny. Moreover, transparency allows individuals to check what personal information has been collected about them.

6.48 In our preliminary consultations it was emphasised that people subject to surveillance should know they are being watched, by whom and for what purpose.[73] It was suggested at a community roundtable that signs should indicate why surveillance is being used, and not merely that surveillance is taking place.[74] The NSWLRC has noted that 'the identity of the user should include an address at which the user can be contacted, otherwise a front name can be used to avoid accountability'.[75] In consultations with Indigenous groups it was also suggested that there needs to be transparency around who has access to footage.[76]

6.49 The commission acknowledges that transparency is not always achievable. For example, while it is reasonable to expect a corner shop to put up signs notifying the public that CCTV is in use, it would seem unreasonable to insist that a person taking a photograph on a mobile phone should always alert the public to his or her actions. In addition, some surveillance practices are deliberately covert, for example, those employed by private investigators or police. In these situations, transparency would detract from the effectiveness of the practice.

6.50 For these reasons, we have confined the applicability of the principle to 'wherever practicable'. An issue for further consideration is whether the prevalence of surveillance in public places means that notification of all surveillance practices would be overwhelming. Notice on this scale may lose its effectiveness.

3. Public place surveillance conducted on a continuous basis should be carried out for a legitimate purpose that is relevant to the activities of the organisation conducting it

6.51 In our preliminary consultations many groups noted the importance of purpose as a guiding principle to control public place surveillance practices.[77] The view was expressed that there should be a 'valid reason' for surveillance,[78] and that users should have to continually justify the surveillance.[79]

6.52 What is a legitimate purpose for surveillance? In 2001, the NSWLRC listed four legitimate uses of overt surveillance:

1) protection of the person
2) protection of property
3) protection of the public interest
4) a catch-all category, 'protection of a legitimate interest'.[80]

6.53 In our Workplace Privacy report, we noted that one way to identify a legitimate purpose is to require a direct connection between an organisation's operations and the surveillance practice, and that the connection not be trivial or incidental.[81] An example of such a connection raised in consultations was that while shopping centres need surveillance for insurance, negligence and safety reasons, they should not be able to use the systems for other purposes.[82] The NSWLRC noted that surveillance cameras in a casino were not being used in a manner appropriate for their purpose when zooming in on female patrons' apparel.[83]

67 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [4.39].

68 Ibid [4.41]–[4.66].

69 *Peck v United Kingdom*, 44647/98 [2003] I Eur Court HR 44, [76].

70 Leon Hempel and Eric Töpfer, *CCTV in Europe: Final Report* (2004) 66–7. The report provides a comparative overview of CCTV use in Austria, Denmark, Germany, Hungary, Norway, Spain and the United Kingdom.

71 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications* LRC 57–1998 (1998).

72 British Columbia Law Institute, *Report on the Privacy Act of British Columbia* BCLI Report No 49 (2008) Rec 3.

73 Roundtable 29.

74 Roundtable 18.

75 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [4.48].

76 Roundtable 28.

77 Roundtables 1, 2, 9, 19, 29.

78 Roundtable 18.

79 Roundtable 18.

80 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [4.44].

81 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [3.47].

82 Roundtable 17.

83 New South Wales Law Reform Commission, *Surveillance: An Interim Report* Report 98 (2001) [4.47].

Chapter 6 Options for Reform

4. Public place surveillance conducted on a continuous basis should be proportional to its legitimate purpose

6.54 The use of surveillance for a legitimate purpose does not justify modes of surveillance that are excessively intrusive relative to the importance of that purpose. For example, an intrusive form of surveillance may be justifiable when designed to protect individuals from grave physical harm, but its use to avoid minor loss of property is likely to be disproportionate. The principle of proportionality also means that a user of surveillance ought to use the least privacy-intrusive means of achieving the purpose.[84]

6.55 Camera placement may be one means of ensuring proportionality. In consultations, it was suggested that there should be some control of where cameras are placed and what they can view.[85] In our Workplace Privacy Report we suggested that it would be disproportionate to aim cameras at staff to deter theft. Instead, we suggested that a proportionate use of cameras would be to aim them at stock.[86]

6.56 As we have suggested above, it is difficult to devise principles to apply to once off surveillance practices. While an individual may believe that they have a legitimate purpose for using a surveillance device, how does the community assess whether that purpose is acceptable? While the current law outlaws some of the most offensive types of surveillance practices, (for instance stalking)[87] is there a need for more regulation?

QUESTIONS: PRINCIPLES TO GUIDE PUBLIC PLACE SURVEILLANCE

1. Do you agree with the draft principles proposed by the commission to guide policy making about public place surveillance?
2. Should the once-off or intermittent use of surveillance practices by individuals be regulated?

OPTIONS FOR REFORM

6.57 We have developed a number of options for reforming the way public place surveillance is regulated in Victoria. The commission has not reached decisions about any of the options described in this chapter which are presented for public discussion.

6.58 These options regulate practices that fall within our definitions of 'public place' and 'surveillance'. We have defined 'public place' as any place to which the public has access as of right or by invitation. We have defined 'surveillance' as any deliberate or purposive monitoring of people whether isolated or systematic that may or may not involve the use of a device. For a variety of reasons which we explained in Chapter 1, we have excluded certain forms of surveillance from our review including:

- surveillance of telephone communications
- various forms of data surveillance, including surveillance in cyberspace
- the use of surveillance by law enforcement officers.

6.59 The draft options which follow are not mutually exclusive. Some, or all, of them could form part of a broad regulatory regime adopted by government in response to the increased use and capacity of public place surveillance.

6.60 In summary the options encompass:

1. ***A role for an independent regulator to monitor, report, and provide information about public place surveillance in Victoria.*** This is a 'light touch' reform option that seeks to increase our knowledge of surveillance practices, as well as educate users and the community about how to comply with existing law and observe industry standards, or observe the proposed best practice voluntary or mandatory standards. The regulator may need statutory powers of investigation and responsibility for reporting to parliament regularly about whether additional regulation is required.

2. ***New voluntary best-practice standards to promote responsible use of surveillance in public places.*** The regulator could be given responsibility for devising best practice voluntary standards which explain the law and promote best practice. Compliance with best-practice voluntary standards could be encouraged by tying them to Victorian government procurement criteria.
3. ***Mandatory codes to govern the use of surveillance in public places with sanctions for non-compliance.*** Mandatory codes could be limited to specified forms of public place surveillance or users (eg, excluding personal use) and could be enforced through criminal or civil penalties. Mandatory codes may be appropriate where there is widespread non-compliance with best practice voluntary standards.
4. ***A licensing system for some surveillance practices.*** Because some surveillance devices or practices have the capacity to be particularly invasive of privacy, the licensing of specified devices or practices may safeguard against abuse.
5. ***Changes to clarify and strengthen the SDA (Vic).*** We suggest a number of changes that would bring the Act in line with current technologies and surveillance practices, resolve uncertainties about the reach of the Act and broaden the enforcement regime.
6. ***A new statutory obligation to refrain from committing a serious invasion of privacy.*** It is arguable that all members of the community should have a legal obligation not to engage in serious invasions of the privacy of others. Under this draft option people aggrieved by serious invasions of privacy would be able to take legal action to enforce their right to privacy.

OPTION 1—AN INDEPENDENT REGULATOR TO MONITOR PUBLIC PLACE SURVEILLANCE

6.61 The commission suggests that consideration be given to providing an appropriate regulator with specific responsibility to:

- monitor the use of surveillance in public places
- monitor the operation and effectiveness of the law
- inform people about how to comply with the law
- to promote observance of proposed voluntary best-practice standards
- to report regularly to parliament about whether regulation of public place surveillance is adequate.

6.62 The case for giving responsibilities of this nature to an independent regulator is strong, particularly because individuals may often be unaware of misuse of public place surveillance as it may be unnoticed or covert.

6.63 There is also a lack of empirical data about the extent of surveillance in public places in Victoria. In particular, there is little information about who uses surveillance, where it is used and for what purposes. Further, there is little information about possible misuse of public place surveillance. An independent regulator would perform a valuable role in collecting this information.

6.64 As we have mentioned earlier, there also appears to be a lack of awareness in the community about existing regulation of public place surveillance.[88] Deficiencies exist in knowledge of relevant laws, about how to use surveillance in privacy-protective ways and about awareness of rights when subjected to surveillance in public places. There seems to be little awareness about who to contact when people have a concern about public place surveillance.[89]

6.65 No regulator has specific responsibility for ensuring compliance with the SDA(Vic), or for monitoring the use of surveillance in public places. The Victorian Privacy Commissioner's current responsibilities in relation to public place surveillance are limited. The Commissioner has supervisory functions only when public sector users, such as police and local councils, engage in surveillance to collect 'private information'.

84 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [3.50].

85 Roundtable 8.

86 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [3.51].

87 *Crimes Act 1958* (Vic) s 21A.

88 Roundtable 22.

89 Roundtables 22, 28.

Chapter 6 Options for Reform

6.66 Consideration should be given to the functions of other regulators when devising responsibilities for the independent regulator. For example, there may be benefit in paying close attention to the functions of the Environmental Protection Authority as the misuse of surveillance in public places arguably threatens the human environment in ways similar to those in which some industrial and domestic activities pollute the physical environment. It has taken some time for us as a society to learn of the advantages in carefully monitoring our physical environment before it is too expensive or too late to take remedial action. The lessons learnt from our management of the physical environment may be useful when considering how we should manage an emerging activity, such as surveillance, which has many benefits but also has the capacity to radically change the way in which we use and enjoy our public places.

Who should be the regulator of public place surveillance?

6.67 Given the established expertise of the Victorian Privacy Commissioner in protecting privacy interests, the Commissioner appears to be an obvious choice to exercise regulatory functions concerning the use of surveillance in public places.[90]

6.68 The Victorian Privacy Commissioner has a number of existing functions in relation to the handling of 'personal information'[91] by Victorian public sector agencies, including educative,[92] audit and review,[93] and monitoring[94] responsibilities. The Commissioner is also empowered to receive and resolve complaints about the handling of personal information by a public sector agency,[95] to issue compliance notices,[96] and to carry out investigations for that purpose.[97] It may be desirable to expand the functions of the Victorian Privacy Commissioner so that they are similar to the broader powers of the Federal Privacy Commissioner.

6.69 The Federal Privacy Commissioner has educative,[98] audit,[99] investigative[100]and complaint-handling[101] functions in relation to interferences with privacy and the handling of personal information by Commonwealth public sector agencies and private organisations (excluding small businesses).[102] The ALRC has recommended that these functions extend to all businesses.[103] It is important to consider whether the proposed regulator should have powers that extend to the private and public sectors.

QUESTIONS: A NEW ROLE FOR AN INDEPENDENT REGULATOR

3. Do you agree with the proposal that an independent regulator should have responsibility for monitoring the use of public place surveillance in Victoria? Who should perform this role?

Specific functions of the regulator

6.70 The specific functions given to an independent regulator of public place surveillance could include the following.

Monitoring and research

6.71 The independent regulator could:

1. collect information and conduct empirical research about surveillance practices in Victoria
2. monitor the operation of existing and proposed regulatory standards and codes
3. monitor the operation of the law in Australia and elsewhere
4. monitor the development of technology in order to ensure that appropriate regulatory regimes are in place
5. identify and monitor regulatory schemes that require, or have an impact on, the use of surveillance in public places (eg, licensing regimes for liquor, gaming, private security, private investigators) and ensure these schemes offer consistent privacy protection
6. review Australian Standards relating to design and use of CCTV and other surveillance technologies.

Registration

6.72 One mechanism to aid the regulator in its monitoring role is to require certain users of public place surveillance, or users of certain forms of surveillance, to register their systems with the regulator.

6.73 Many European countries require some users of public place surveillance to notify or register with a regulator.[104] Observers have suggested that notification may be important for effective enforcement of existing law. In their study of video surveillance in Norway and Denmark, Carsten Wiecek and Ann Rudinow Sætnan noted the ease with which the Norwegian regulator conducted inspections of registered enterprises with video surveillance (approximately 400) in contrast to the Danish regulator's reliance on complaints brought to its attention.[105] In addition, we note that the UK Information Commissioner has said that registration promotes transparency and openness[106] and is one of the draft principles for surveillance regulation devised by the Commission.

6.74 A registration system could include exemptions for certain users of public place surveillance systems. The European Union Data Protection Directive provides exemptions for notification requirements under specified conditions.[107] In addition, notification requirements, like many other provisions in the Directive, do not apply to activities undertaken solely for journalistic purposes or for the purpose of artistic or literary expression.[108] In the UK, notification exemptions are available to non-profit organisations and others.[109] Alternatively, one could require organisations to register particularly invasive surveillance systems only.

6.75 How would a registration requirement affect a public place surveillance user such as a business using CCTV? In the UK, the Data Protection Act requires that 'data controllers' notify the Information Commissioner about their processing of personal data.[110] Most uses of CCTV by businesses and organisations amount to data collection under the Act.[111] Data controllers can notify the Commissioner that they process personal data via the internet, by completing a form, or by telephone.[112] According to the Information Commissioner, an attempt has been made to keep the process simple and it is not intended that:

> *the register should contain very detailed information about a data controller's processing. The aim is to keep the content at a general level, with sufficient detail to give an overall picture of the processing.'*[113]

90 This step is in keeping with other jurisdictions where the same entity monitoring compliance with information privacy laws also monitors the use of surveillance.

91 Personal information is defined in s 3 of the *Information Privacy Act* 2000 (Vic) as information or an opinion (including information or an opinion forming part of a data base), that is recorded in any form and whether true or not, about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion. It does not include information that the *Health Records Act* 2001 (Vic) applies to.

92 *Information Privacy Act 2000* (Vic) s 58(o).

93 *Information Privacy Act 2000* (Vic) ss 58(g), 58(j).

94 *Information Privacy Act 2000* (Vic) s 58(k).

95 *Information Privacy Act 2000* (Vic) pt 5.

96 *Information Privacy Act 2000* (Vic) pt 6.

97 *Information Privacy Act 2000* (Vic) s 34.

98 *Privacy Act 1988* (Cth) s 27(1)(m).

99 *Privacy Act 1988* (Cth) s 27(1)(h).

100 *Privacy Act 1988* (Cth) ss 27(1)(a), 40.

101 *Privacy Act 1988* (Cth) s 36.

102 Defined as businesses with an annual turnover of $3 million or less: *Privacy Act 1988* (Cth) s 6D(1)–(2).

103 See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) Rec 39–1.

104 This is pursuant to Article 18 of the European Union Data Protection Directive which requires organisations to notify the public authority monitoring application of the Directive of any automatic processing of personal data. The European Parliament and the Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31. Further details are provided in Chapter 5.

105 Carsten Wiecek and Ann Rudinow Sætnan, *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark* (2002) 22–3.

106 Information Commissioner's Office, 'Notification Handbook: A Complete Guide to Notification' (2007) *Information Commissioner's Office [ICO]* 1.

107 The European Parliament and the Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31, art 18(2)–(5).

108 The European Parliament and the Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31, art 9.

109 Information Commissioner's Office [UK], *Do I Need to Notify?* <www.ico.gov.uk/what_we_cover/data_protection/notification/do_i_need_to_notify.aspx> at 18 November 2008.

110 Information Commissioner's Office, 'Notification Handbook: A Complete Guide to Notification' (2007) *Information Commissioner's Office [ICO]* 4.

111 Information Commissioner's Office [UK], *CCTV Code of Practice* (Revised edition 2008) 5.

112 Information Commissioner's Office, 'Notification Handbook: A Complete Guide to Notification' (2007) *Information Commissioner's Office [ICO]* 4.

113 Ibid 1.

Chapter 6 Options for Reform

Improving public and user awareness

Information and training

6.76 The independent regulator could also provide information and training programs to the public to increase awareness of public place surveillance about matters such as:

1. how surveillance is used in public places and for what purposes
2. any restrictions that should apply to the use of particular surveillance devices
3. the risks and benefits of surveillance practices
4. how the current law regulates surveillance practices and how to comply with it
5. how surveillance in public places could be used in ways that are protective of privacy
6. how to observe industry standards or observe the proposed best practice voluntary or mandatory standards.

Advisory guidelines

6.77 Our preliminary consultations revealed that the terms of the SDA (Vic) are not widely understood. Consideration should be given to providing the proposed regulator with the power to develop advisory guidelines to explain the SDA (Vic) and other relevant laws. These guidelines could be taken into account by the regulator or a court when considering whether there has been a breach of the law.

6.78 The Federal Privacy Commissioner has issued guidelines to help organisations comply with the Privacy Act (Cth).[114] The guidelines are not legally binding, but may be taken into account by the Commissioner in the handling of a complaint.[115] Similarly, the Victorian Privacy Commissioner has issued guidelines to help Victorian agencies comply with the IPA (Vic).[116]

6.79 The ALRC recently recommended that the Federal Privacy Commissioner (OPC) issue technology-specific guidance that would be non-binding[117] but would 'indicate the OPC's understanding of the requirements set out in the privacy principles'.[118] In formulating the guidelines, the ALRC suggests that the OPC look at similar guidance published overseas, such as the Ontario Privacy Guidelines for RFID systems, and the UK CCTV code of practice.[119]

6.80 Guidelines are used in many areas. For example, the Victorian WorkSafe Authority is empowered to develop 'compliance codes' to provide practical guidance to persons having duties or obligations under the *Occupational Health and Safety Act* 2004 (Vic) (OHS Act (Vic)).[120] The NSW Anti-Discrimination Board can develop and promote 'codes of practice' about the operation of equal opportunity laws. While the codes are not legally binding, the President of the Board and the Administrative Decisions Tribunal may take compliance with them into account when exercising their functions under the Act.[121]

Powers of investigation

6.81 The regulator could also be given the power to carry out investigations into the use of surveillance in public places. This power would assist the regulator to gather empirical data and to monitor public place surveillance by public and private sector organisations. The investigatory power could exercised in response to concerns raised by members of the community or on the regulator's own motion.

6.82 There are three broad categories of investigatory powers: the power to require people to answer questions; the power to compel the production of documents; and the power to enter and search premises. The investigatory powers of many oversight bodies are limited to the power to obtain information and documents only.[122] The power to enter and search premises is reserved for the most heavily regulated areas. Further, where oversight bodies are provided with entry and search powers, they may need to obtain authorisation from a judge or magistrate to use these powers.[123]

6.83 The Victorian Privacy Commissioner's current investigative power is limited to her complaint-handling function.[124] She is also empowered to examine (including on her own motion) the practices of an organisation with respect to personal information maintained by the organisation, whether the information is maintained according to the privacy

principles in Victorian privacy legislation[125] and the impact on personal privacy of any act or practice of a public sector organisation.[126] However, her power to obtain documents and information is limited to matters raised by a complaint.[127]

6.84 Providing own motion investigatory powers to the regulator would enable the regulator to better understand underlying systemic problems. A number of other regulators have own-motion investigatory powers that include powers to obtain information and documents. For example, the Federal Privacy Commissioner has the power to initiate own-motion investigations about potential breaches of privacy, not limited to a matter raised in a complaint,[128] the power to obtain information and documents relevant to an investigation,[129] and the power to enter premises to inspect documents in some circumstances.[130] The NSW Privacy Commissioner also has power to conduct inquiries and make investigations into privacy related matters on her own motion,[131] and the power to obtain information and documents, subject to some limitations.[132] Other oversight and regulatory bodies have broad investigative powers within their jurisdictions, for example the Victorian Commissioner for Law Enforcement Data Security (CLEDS),[133] the Australian Securities and Investments Commission (ASIC),[134] the Australian Competition and Consumer Commission (ACCC),[135] and the Safety, Rehabilitation and Compensation Commission (SRCC).[136]

Reporting to Parliament

6.85 The regulator could be empowered to report to parliament about any matters arising in connection with his or her monitoring functions and to make recommendations for legislative reform. In addition, the regulator could have the power to recommend that any report about public place surveillance be tabled in parliament. This would enable the regulator to keep the community informed about relevant issues, including developments in surveillance technology, the effectiveness of the law, the number of complaints, and problems of a systemic nature.

6.86 The Victorian Privacy Commissioner currently has limited reporting powers. The Commissioner may report to the Attorney-General in relation to:

- the commission's examination and assessment of proposed legislation that would otherwise interfere with or have an adverse effect on the privacy of an individual[137]
- the commission's research and monitoring of developments in data processing and computer technology with potential adverse effects on personal privacy [138]
- any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of personal privacy'[139]
- any act or practice the Commissioner considers to be an interference with privacy whether or not a complaint has been made.[140]

The Act does not require the Minister to table the reports in Parliament.

6.87 In contrast, the Federal Privacy Commissioner is empowered to provide the Minister with a report relating to an inquiry or audit and the Minister must provide a copy of the report to parliament.[141] The NSW Privacy Commissioner also has the power to make a special report to parliament on any matter arising in connection with his or her functions, and may include a recommendation that the report be made public immediately.[142]

114 Office of the Federal Privacy Commissioner, *Guidelines to The National Privacy Principles* (2001).

115 Ibid 4.

116 Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles* Guidelines edition.02 (2006); Office of the Victorian Privacy Commissioner, *Short Guide to the Information Privacy Principles* (2006).

117 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [4.56].

118 Ibid [10.52].

119 Both of which are voluntary guidelines: Ibid [10.53].

120 *Occupational Health and Safety Act 2004* (Vic) s 149.

121 *Anti-Discrimination Act 1977* (NSW) ss 4, 120A.

122 For example, the Victorian Privacy Commissioner and the CLEDS do not have entry and search powers.

123 See, eg, *Trade Practices Act 1974* (Cth) ss 154 X, 154Y.

124 See *Information Privacy Act 2000* (Vic) ss 58(i) and 34.

125 *Information Privacy Act 2000* (Vic) s 58(g).

126 *Information Privacy Act 2000* (Vic) s 58(t).

127 *Information Privacy Act 2000* (Vic) s 34.

128 *Privacy Act 1988* (Cth) s 40(2).

129 *Privacy Act 1988* (Cth) s 44.

130 *Privacy Act 1988* (Cth) s 68.

131 *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(l).

132 *Privacy and Personal Information Protection Act 1998* (NSW) s 37(1)–(2).

133 Under the *Commissioner for Law Enforcement Data Security Act 2005* (Vic) s 12(1).

134 Under the *Australian Securities and Investments Commission Act 2001* (Cth) s 13.

135 Under the *Trade Practices Act 1974* (Cth) s 155 ('Power to obtain information, documents and evidence').

136 Under the *Occupational Health and Safety Act 1991* (Cth) s 40.

137 *Information Privacy Act 2000* (Vic) s 58(l).

138 *Information Privacy Act 2000* (Vic) s 58(m).

139 *Information Privacy Act 2000* (Vic) s 58(n).

140 *Information Privacy Act 2000* (Vic) s 63(1). The Minister *may* table such a report in parliament: *Information Privacy Act 2000* (Vic) s 63(2).

141 *Privacy Act 1988* (Cth) s 32(1), (3).

142 See *Privacy and Personal Information Protection Act 1998* (NSW) s 65(1)–(2). Other entities with reporting power include the NSW Ombudsman who under the *Surveillance Devices Act 2007* (NSW) ss 48–9 must from time to time inspect the records of each law enforcement agency to determine the extent of compliance with the Act and to make a report to the Minister on the results of an inspection, which the Minister must provide to Parliament. Under the *Commissioner for Law Enforcement Data Security Act 2005* (Vic) s 13, the Commissioner for Law Enforcement Data Security (CLEDS) has the power to disclose any information obtained or received through exercise of his or her functions to the Director of Police Integrity, or the Privacy Commissioner for further action.

Chapter 6 Options for Reform

QUESTIONS: SPECIFIC FUNCTIONS OF THE REGULATOR

4. Should the regulator be given the functions proposed by the commission?
5. Are there any other functions that should be given to the regulator?
6. Would a registration scheme assist the regulator to acquire information about surveillance use? Is such a scheme practical? Should some users be exempt from registration requirements?
7. What (if any) investigatory powers should be given to the regulator?
8. Should the regulator have an own motion investigatory power in order to identify systemic problems with surveillance in public places?
9. Should the regulator have the power to develop advisory guidelines which explain the law concerning surveillance in public places?

OPTION 2—NEW VOLUNTARY BEST-PRACTICE STANDARDS TO PROMOTE RESPONSIBLE USE OF SURVEILLANCE IN PUBLIC PLACES

6.88 Consideration should be given to providing the independent regulator with the power to develop voluntary best-practice standards to guide users about appropriate forms of conduct when using surveillance devices in public places. While the regulator would have on-going responsibility for developing and publishing standards for all users of surveillance devices, it is unlikely that casual users would be aware of voluntary standards. The regulator would be expected to monitor compliance with the voluntary best-practice standards as well as compliance with the law. The regulator could be assisted in this task by the proposed monitoring and investigative powers mentioned earlier.

6.89 At present, some users of surveillance comply with their own standards or with those developed by industry groups. In a few instances, government departments have published best-practice standards to assist users of particular devices. For example, the Department of Justice has issued a CCTV Toolkit for Victoria intended for a broad audience including local councils, traders, urban planners and all those using CCTV for purposes including crime reduction, and the promotion of 'safe shopping, transport and entertainment places.'[143] The Toolkit recommends that a series of steps be undertaken before a CCTV system is installed. These include the determination of policy objectives and community consultation. It also recommends any decision to install CCTV should be accompanied by in-house documentation outlining legal, administrative and technical requirements.[144] The Victorian Privacy Commissioner has also issued information sheets on other forms of public place surveillance, including mobile telephone cameras and GPS.[145]

6.90 The Council of Australian Governments (COAG) code of practice for the use of CCTV in mass passenger transport aims to ensure that these systems contribute to counter-terrorism measures. It also includes a discussion about the need to respect the privacy expectations of the public by giving notice of CCTV and by ensuring that collected images are used only for the purpose for which they are intended.[146]

6.91 An example of a voluntary regulation scheme are the 'compliance codes' approved by the Minister for WorkCover for the purposes of providing practical guidance to employers on how to ensure that workplaces will secure the health, safety and welfare of employees and other people at work.[147] WorkSafe Victoria has devised a number of codes[148] which are designed to be used in conjunction with the OHS Act (Vic) and regulations. Failure to comply with a compliance code does not give rise to any civil or criminal liability, but a person who complies with a compliance code is taken to have complied with the Act.[149] A WorkSafe Authority Inspector can cite an approved industry code of practice when indicating the measures that should be taken to remedy an alleged contravention or non-compliance. Failure to comply with a requirement in an improvement or prohibition notice is an offence.[150]

6.92 Voluntary standards developed by the regulator for public place surveillance could draw upon the draft principles devised by the commission. Different voluntary standards could be developed for different forms of surveillance practices. The standards should be developed in consultation with users, key stakeholders and the broader community.

6.93 The voluntary standards would encourage people to undertake surveillance activities in public places in a responsible manner by bearing in mind privacy considerations as well as protection or furtherance of their own interests. Drawing upon the draft principles devised by the commission, some of the matters that could be included in voluntary standards are:

- taking active measures, such as monitoring of staff responsible for the use of surveillance systems, in order to minimize privacy invasion
- ensuring that the public receives adequate notice about the surveillance, including who is responsible for the system, why it is being used, and who to contact about complaints
- clear identification of the purpose of a public place surveillance system[151]
- regularly evaluating the surveillance practice to determine if it continues to be justified and proportionate
- consultation with communities likely to be affected by the surveillance in some circumstances.

6.94 If the regulator becomes aware of widespread non-compliance with voluntary standards, he or she could report the matter to parliament and recommend that all or part of the regime become mandatory or that additional effort be devoted to informing the community about the voluntary standards.

Procurement

6.95 One possible tool to encourage compliance with a voluntary standard is to make compliance a condition of doing business with the Victorian government.[152] A condition to this effect may be added to government 'procurement policies' without the need for legislation.[153] Additionally, compliance with voluntary codes could be built into selection criteria for organisations that sit on government panels or adherence with a voluntary standard could be tied to eligibility for government funding.

6.96 An example of a current procurement policy is the *Environmental Procurement Policy*, which provides guidance for Victorian government departments on how to embed environmental considerations into procurement decisions. This policy requires government departments to purchase 10 per cent of their electricity in the form of Green Power.[154]

6.97 There is a similar mechanism in the standards for the security and integrity of law enforcement data systems. Victoria Police is required to ensure that agreements with third parties 'include the requirement that information security responsibilities be addressed in job descriptions or in relevant background documentation provided for positions that will require access to law enforcement data.'[155]

QUESTIONS: VOLUNTARY BEST-PRACTICE STANDARDS

10. Would voluntary best-practice standards developed or approved by the regulator be useful?
11. Is linking voluntary best-practice standards to government procurement criteria a good strategy for encouraging responsible use of surveillance practices? Are there other strategies for encouraging compliance with the voluntary standards?

OPTION 3—MANDATORY CODES OF PRACTICE

6.98 The independent regulator could be given the power to develop mandatory codes of practice that bind some or all public place surveillance users. Unlike voluntary standards or advisory guidelines, non-compliance with mandatory codes would result in some form of sanction. The mandatory code of practice could apply to particular surveillance practices or particular users. There could be, for example, a mandatory *CCTV Code of Practice* or a mandatory *Code of Practice for Users of Tracking Devices*.

6.99 There are many examples of mandatory codes in Australian legislation. The *Disability Discrimination Act 1992* (Cth) gives the Commonwealth Attorney-General the power to make standards about various matters concerning access to services and facilities by

143 Department of Justice, Victoria, *CCTV Toolkit for Victoria: Is CCTV the Best Response?* (2007) 2. The commission notes that this document is no longer available on the Department of Justice website.

144 Ibid 12.

145 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003); Office of the Victorian Privacy Commissioner, *Privacy and Global Positioning System Technology*, Info Sheet 02.08 (2008).

146 Council of Australian Governments, *A National Approach to Closed Circuit Television: National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (2006).

147 *Occupational Health and Safety Act 2004* (Vic) s 149.

148 Including, for example, codes relating to hazardous substances, confined spaces and the prevention of falls: *Occupational Health and Safety Regulations 2007* (Vic) ch 3.

149 *Occupational Health and Safety Act 2004* (Vic) ss 150, 152.

150 *Occupational Health and Safety Act 2004* (Vic) ss 62, 111–2.

151 Including by showing that there is a pressing need for the surveillance, that it will be used for a legitimate purpose, that it is proportionate to the problem it is being used to address and that less privacy invasive measures are not practicable.

152 The commission notes the Victorian Equal Opportunity and Human Rights Commission have recommended the use of procurement policies as a compliance tool: Victorian Equal Opportunity and Human Rights Commission, *Submission to Equal Opportunity Review: Discussion Paper 2007* (2008) 66–7.

153 Ibid 66.

154 Victorian Government Purchasing Board, *Environmental Procurement Policy* <www.vgpb.vic.gov.au/CA256C450016850B/0/D05DD7274E35CE40CA2571E3000C39D4?OpenDocument> at 30 January 2009.

155 Commissioner for Law Enforcement Data Security, *Standards for Victoria Police: Law Enforcement Data Security* (2007) Protocol 4.1, 16.

Options for Reform

people with a disability.[156] The Attorney-General has used the power to make *Disability Standards for Accessible Public Transport* and *Disability Standards for Education*.[157] These standards operate as a form of delegated legislation. It is unlawful to contravene a disability standard.[158]

6.100 Another example is the *Occupational Health and Safety Code of Practice 2008* (Cth), which has been approved by the Minister under the OHS Act (Cth).[159] The code is designed to provide practical guidance to employers on safe work practices and risk management in relation to hazards. The code is admissible as evidence in proceedings,[160] and a breach of the code will be taken to be a breach of the Act.[161]

6.101 Mandatory codes are obviously far more onerous than voluntary standards because non-compliance attracts a sanction. In its recent report on privacy law the ALRC decided not to recommend mandatory codes[162] to expand upon privacy principles in the Privacy Act (Cth).[163] The ALRC referred to submissions that binding codes would not be appropriate for a light touch regime such as the Privacy Act (Cth)[164] and might create too high a compliance burden on organisations.[165]

6.102 Mandatory codes of practice have the advantage that people are more likely to comply with them than with voluntary standards. Mandatory codes may be a suitable way of regulating particularly invasive surveillance practices. An example may be the x-ray machines at airports which provide the operator with an unclothed image of passengers. Mandatory codes might also be appropriate for users who share surveillance information once it is collected, or large-scale users of surveillance such as shopping centres and sporting venues.

Industry developed mandatory codes

6.103 If mandatory codes are adopted, it may be desirable to permit particular user-groups to develop their own codes which would take the place of a specific generic code if approved by the regulator. A code of this nature might be developed where a particular industry uses a surveillance practice in a certain way for example, the security industry's use of CCTV.

6.104 Industry devised mandatory codes are currently used in a number of areas of activity. For example, the Federal Privacy Commissioner and the Victorian Privacy Commissioner have the power to approve codes in substitution for compliance with relevant information privacy principles.[166] The Commissioners must be satisfied that the code is at least as stringent as the applicable privacy principles.[167]

6.105 The *Biometrics Institute Privacy Code* is an example of a code approved under the Privacy Act.[168] The principles in this code are substantially the same as the privacy principles in the Privacy Act (Cth). Where they differ they 'intend to provide additional privacy protection to end-users,'[169] including, for example, the requirement that wherever practicable, biometric information must be encrypted after collection.[170]

Enforcement options for mandatory codes

6.106 It is necessary to consider the way in which mandatory codes could be enforced.

Complaints-based mechanism

6.107 One enforcement option would be to permit the regulator to act upon complaints made by people who claim to have been harmed by conduct that breaches a mandatory code. The regulator's powers could be modelled on those of the Victorian Privacy Commissioner who has the power to receive complaints and issue compliance notices about information privacy matters.[171]

6.108 The Victorian Privacy Commissioner is empowered to receive and resolve complaints about the handling of personal information by a state public sector agency.[172] The Commissioner may decline to hear a complaint or dismiss a complaint in some circumstances.[173] The commissioner must try to resolve a complaint by conciliation.[174] When a complaint is not successfully resolved at conciliation, or the Commissioner decides that the matter is not suitable for conciliation, the complainant must be given the opportunity to ask the Victorian Civil Appeals Tribunal (VCAT) to determine the complaint.[175] A matter may also

be referred to VCAT directly by the Minister if the Minister believes that the complaint raises an important issue of public policy.[176]

6.109 If a matter is referred to VCAT, the tribunal may issue a number of orders including: an order restraining future conduct, an order to redress loss or damage, payment not exceeding $100,000, payment of the costs of the complaint process, and the correction of personal information.[177]

6.110 The Commissioner is empowered to serve compliance notices requiring a party to take specified action to comply with the privacy principles or an applicable code of practice.[178] A compliance notice can be issued only if the conduct is a serious or flagrant contravention of the principles (or code) or the organisation has engaged in the conduct on at least five separate occasions in the previous two years.[179] It is an offence not to comply with a compliance notice.[180] Only a member of the police force, the Privacy Commissioner or someone authorised by the Commissioner may commence proceedings for an offence under the IPA (Vic).[181]

6.111 A shortcoming of any complaints based enforcement mechanism in relation to public place surveillance, is that in many instances an individual may not be aware that a code has been breached by surveillance practices because many surveillance practices are covert. This problem may be dealt with by providing the regulator with an 'own-motion' investigative power.

Sanctions for non-compliance with mandatory codes

6.112 Civil penalties may be an appropriate way of dealing with breaches of a mandatory code. A civil penalty differs from a criminal penalty. It has a lower standard of proof and there is no finding of criminal culpability. A civil penalty can be supplemented by other sanctions, such as suspension of a licence or an injunction to restrain future conduct.[182]

6.113 In its 2008 Privacy Report, the ALRC recommended the Privacy Act be amended to allow the Privacy Commissioner to seek a civil penalty in the Federal Court or the Federal Magistrates Court when there had been a serious or repeated interference with the privacy of an individual.[183]

6.114 Civil penalties have been used as an enforcement tool in a variety of contexts, particularly when government has taken the view that it should play a role in ensuring compliance with the law, but the conduct in question should not be characterised as criminal. As the ALRC has observed, 'Parliament should exercise caution about extending the criminal law into regulatory areas unless the conduct being

156 *Disability Discrimination Act 1992* (Cth) s 31.The Australian Human Rights Commission (formerly the Human Rights and Equal Opportunity Commission) advises the Attorney-General about the content and operation of the disability standards: *Disability Discrimination Act 1992* (Cth) s 67(1)(d)–(e).

157 *Disability Standards and Guidelines* (2008) Australian Human Rights Commission <http://www.hreoc.gov.au/disability_rights/Standards/standards.html> at 2 February 2009.

158 *Disability Discrimination Act 1992* (Cth) s 32.

159 *Occupational Health and Safety Act 1991* (Cth) s 70.

160 *Occupational Health and Safety Act 1991* (Cth) s 71(a).

161 Unless the court is satisfied that the person complied with the relevant provision of the Act or regulations in ways other than by observing the code of practice: *Occupational Health and Safety Act 1991* (Cth) s 71(b).

162 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 2: Final Report* 108 (2008) [48.34].

163 Ibid [48.20].

164 Ibid [48.27], citing Australian Government Department of Employment and Workplace Relations, *Submission PR 211* (27 February 2007); National Health and Medical Research Council, *Submission PR 114* (15 January 2007).

165 Ibid [48.31], citing Australian Compliance Institute, *Submission PR 419* (7 December 2007); Investment and Financial Services Association, Submission PR 538 (21 December 2007); National Australia Bank, *Submission PR 408* (7 December 2007).

166 *Privacy Act 1988* (Cth) s 18BB(7); *Information Privacy Act 2000* (Vic) s 18(3)(d).

167 *Privacy Act 1988* (Cth) s 18BB(2)(a); *Information Privacy Act 2000* (Vic) s 18(2)(a).

168 This code, and other codes approved under privacy legislation are discussed in detail in Chapter 5.

169 Biometrics Institute, *Biometrics Institute Privacy Code* (2006) 1.

170 Ibid 16–18.

171 Under Parts 5 and s 44 of the *Information Privacy Act 2000* (Vic).

172 The range of bodies that the Commissioner can hear a complaint against includes local councils, statutory bodies, state Ministers and parliamentary secretaries and in some cases organisations that provide services to the state: *Information Privacy Act 2000* (Vic) s 9.The complaint handling powers of the Commissioner are found in Part 5 of the *Information Privacy Act 2000* (Vic).

173 *Information Privacy Act 2000* (Vic) s 29, s 30.

174 *Information Privacy Act 2000* (Vic) s 33.

175 *Information Privacy Act 2000* (Vic) ss 37, 32.

176 *Information Privacy Act 2000* (Vic) s 31

177 *Information Privacy Act 2000* (Vic) s 43.

178 *Information Privacy Act 2000* (Vic) s 44 (1)(a).

179 *Information Privacy Act 2000* (Vic) s 44 (1)(b).

180 *Information Privacy Act 2000* (Vic) s 48.

181 *Information Privacy Act 2000* (Vic) s 71.

182 Australian Law Reform Commission, *Securing Compliance: Civil and Administrative Penalties in Federal Regulation* (2002) <www.alrc.gov.au/media/2002/mb0523.htm> at 5 February 2009.

183 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) Rec 50-2.

proscribed is clearly deserving of the moral censure and stigma that attaches to conduct deemed criminal.'[184] The ALRC has also noted that the lower burden of proof—the balance of probabilities as opposed to proof beyond reasonable doubt—and greater procedural flexibility makes civil penalties an attractive regulatory tool for legislators.[185]

6.115 Criminal offences already exist for the most offensive forms of surveillance and behaviours incidental to surveillance. For example, the *Crimes Act 1958* (Vic) makes it an offence punishable by up to 10 years imprisonment to stalk another person with the intention of causing them physical or mental harm, or to fear for their safety.[186] Section 17 of the *Summary Offences Act 1966* (Vic) makes it an offence to engage in behaviour that is 'indecent, offensive or insulting' in or near a public place. Since September 2007 'upskirting' is a separate offence.[187]

6.116 While civil penalties may be the most appropriate remedy for a breach of a mandatory code, it is necessary to consider whether behaviour that is repeated or wilful warrants a criminal sanction. It may be appropriate to introduce criminal sanctions for escalating conduct if the regulator identifies that it is a recurring problem.

QUESTIONS: MANDATORY CODES OF PRACTICE

12. Should there be mandatory codes, if so, what conduct should they regulate?
13. If mandatory codes are introduced, should the regulator have the power to approve industry codes that operate in their place?
14. Should the regulator be empowered to investigate complaints made about potential breaches of a mandatory code? How broad should any such powers be?
15. What kind of sanctions should be imposed for breaches of a mandatory code?

OPTION 4—A LICENSING SYSTEM FOR SOME SURVEILLANCE PRACTICES

6.117 Because some surveillance devices or practices have the capacity to be particularly invasive of privacy, a safeguard against abuse may be to require users of specified devices or practices to be licensed. Licensing specified forms of public place surveillance would mean that some practices would be prohibited unless approved by the regulator. A licensing system would also provide the regulator with information about the type and location of systems which would aid the regulator's proposed monitoring role.

6.118 Any licensing system should operate only in relation to those forms of public place surveillance most likely to lead to abuse. Examples include:

- covert surveillance
- CCTV surveillance involving zooming or operator monitoring
- x-ray body scanners
- facial recognition technology
- infra-red, high sensitivity equipment, and systems operating outside the visible light spectrum
- miniature and micro-engineered devices designed for covert surveillance.[188]

6.119 In Norway users of CCTV systems who record sensitive information[189] must obtain a licence before doing so.[190] In Germany, any proposed use of video surveillance data must be registered with the relevant data protection authority,[191] which will conduct an examination of the purpose and proposed installation of the video surveillance system. Once approved, the video surveillance system may be installed but limitations will be imposed on its use. These include that data collected must be kept confidential[192] and any data no longer necessary for the purpose for which the surveillance was permitted must be immediately erased.[193]

6.120 In Sweden, the law requires users of public place surveillance to obtain a permit from the County Administrative Board.[194] However, some users, such as a post office, bank or store which uses surveillance to cover entrances, exits and cash points, are merely required to notify the Board in order to obtain a permit.[195] Otherwise, approval is given only if the

surveillance system is used for crime prevention and detection, and the user's interest outweighs the interests of individuals subject to the surveillance. Individuals who may be affected by the proposed surveillance activity must be heard before a permit is granted.[196]

QUESTIONS: A LICENSING SYSTEM FOR SOME SURVEILLANCE PRACTICES

16. Should users of some forms of surveillance be required to obtain a licence from a regulator?
17. Are there any surveillance practices in Victorian public places that are particularly concerning? If so why?

OPTION 5—CHANGES TO CLARIFY AND STRENGTHEN THE SDA (VIC)

6.121 A number of amendments could be made to clarify some provisions in the SDA, to broaden its coverage and to strengthen its enforcement regime. At present the SDA (Vic) prohibits certain uses of surveillance devices and it permits other uses by implication because the Act says nothing about them. The prohibited practices attract serious criminal sanctions. This regime may not be a particularly effective way of regulating a complex activity like public place surveillance because it is open to the criticism that it is too blunt. In some instances judgements may need to be made about context in order to decide whether particular public surveillance activities should be unlawful.

Expressly prohibiting optical surveillance in certain 'no-go' areas such as toilets, shower areas and change rooms

6.122 At present, the SDA (Vic) prohibits use of an *optical surveillance device* to monitor 'private activities', defined in the Act as those activities where parties may reasonably expect that they may not be observed by someone else, without consent. The explanatory memorandum to the Act suggests that the prohibition extends to activities in toilet cubicles, shower areas and change rooms claiming that:

> *Circumstances in which the parties to an activity may reasonably expect that they may not be observed by someone else include:*
>
> - *activities in toilet cubicles and shower areas;*
> - *activities in change rooms*[197]

6.123 There is, however, uncertainty about the reach of this prohibition because usually a person would reasonably expect to be seen by others when using communal facilities.[198] This uncertainty is evidenced by the fact that some fitness centres have

184 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* Report No 95 (2002) [3.106]. Some regulatory theorists also warn against the over-use of the criminal law in the regulatory area. See, eg, ibid [3.36] citing Mirko Bagaric, 'The "Civil-isation" of the Criminal Law' (2001) 25(4) *Criminal Law Journal* 184, 184–5; Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (1999) 36; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992) 36.

185 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* Report No 95 (2002) [2.81].

186 *Crimes Act 1958* (Vic) s 21A.

187 *Summary Offences Act 1966* (Vic) div 4A. Penalties include three months imprisonment for observing a person's genital or anal areas from beneath and two years imprisonment for visually capturing or distributing images of a person's genital or anal region: *Summary Offences Act 1966* (Vic) ss 41A, 41B and 41C. We discuss these and other provisions in Chapter 5.

188 In 1995, Privacy International called for a prohibition or other restriction on the use of these last three categories of devices: Privacy International, *Privacy International Statement on CCTV Surveillance*, 15 October 1996 <www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61926> at 1 July 2008.

189 *Personal Data Act* (Norway) s 33 ('A licence from the Data Inspectorate is required for the processing of sensitive personal data'); Sensitive personal data is defined in s 2(8) of that Act as: '(a) racial or ethnic origin, or political opinions, philosophical or religious beliefs, (b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, (c) health, (d) sex life, (e) trade-union membership.'

190 Carsten Wiecek and Ann Rudinow Sætnan, *Restrictive? Permissive? The Contradictory Framing of Video Surveillance in Norway and Denmark* (2002) 16.

191 *Bundesdatenschutzgesetz* [Federal Data Protection Act], 1990 (Germany) s 4d. Enforcement of the provisions of the BDSG (including s 6b) and examination of the purpose and practice of video surveillance systems is shared by both the Federal and State the Data Protection Commissions: Letter from Susanne Bohn, Der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit [Federal Commission for Data Protection and Freedom of Information [Germany]] to Victorian Law Reform Commission, 28 November 2008.

192 *Bundesdatenschutzgesetz* [Federal Data Protection Act], 1990 (Germany) s 5.

193 Letter from Susanne Bohn, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [Federal Commission for Data Protection and Freedom of Information [Germany]] to Victorian Law Reform Commission, 28 November 2008.

194 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007) 917.

195 Ibid.

196 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 (2/3) *Surveillance & Society* 216, 223.

197 Explanatory Memorandum, Surveillance Devices Bill 1999 (Vic) cl 3.

198 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003) 4.

Chapter 6 Options for Reform

independently instituted policies to ban mobile telephones in such areas.[199] The Victorian Privacy Commissioner has queried whether the comment in the explanatory memorandum to the SDA (Vic) is an accurate description of the terms of the Act:

> *While courts can take note of the explanatory memoranda to statutes, courts might be reluctant to impose criminal liability for conduct that does not clearly fall within the terms of the Surveillance Devices Act, as currently drafted. It may be better to state explicitly in the Surveillance Devices Act that private activities do occur in certain public places and that invading the privacy of persons in those places is prohibited, with serious penalties for breach.*[200]

6.124 Consideration should be given to amending the SDA to include an express prohibition on the use of all optical surveillance devices in toilet areas, shower areas, and change rooms. As with other prohibitions in the SDA (Vic), this prohibition would not apply to law enforcement officers acting under warrant. For example, we suspect that police might engage in surveillance in such areas to investigate drug related activities and suspected paedophiles.[201]

6.125 A prohibition of this nature appears to be in keeping with public expectations that these are 'no go areas' where all surveillance is regarded as unacceptable.[202] Many international codes of practice and guidelines[203] prohibit or greatly restrict[204] surveillance in such areas.

6.126 This reform proposal parallels our recommendation in the Workplace Privacy report that employers should be prohibited from using optical surveillance and listening devices to monitor the activities of workers in toilets, change rooms, lactation rooms, and washrooms.[205] The Victorian parliament adopted that proposal in 2006 by inserting section 9B in the SDA (Vic).

Extending the SDA's prohibitions to any device capable of tracking

6.127 The SDA (Vic) provides that a device is a 'tracking device' when its 'primary purpose…is to determine the geographical location of a person or an object'.[206] It may be appropriate to amend the definition of 'tracking device' in the SDA (Vic) so that it includes all devices that have the capacity to track, regardless of their primary purpose. Such a change would bring the SDA (Vic) in line with NSW legislation where the prohibition on the use of a tracking device is not limited to devices whose primary purpose is tracking.[207] The express or implied consent of a person being tracked, or being in lawful possession or control of an object being tracked, would continue to act as an exception to the prohibition.[208]

6.128 Changing the definition of tracking devices may have implications for law enforcement agencies by requiring them to obtain warrants in circumstances where currently they do not have to do so. One significant category of device not designed primarily for tracking, but used by police for that purpose is the mobile phone.[209]

Extending the SDA's prohibitions to cover more types of devices

6.129 The SDA (Vic) is currently limited to four types of devices: listening devices, optical surveillance devices, tracking devices, and data surveillance devices.[210] These categories have been overtaken by technological developments and are now incomplete. An example of a surveillance device that does not neatly fit into one of the existing categories is the use of thermal infra-red scanners at airports to detect the body temperature of passengers to control the bird flu pandemic.[211] Another example is the use of walk-in scanners at prisons that test visitors for residue of narcotics or explosives.[212]

6.130 The SDA could be amended to include a new 'catch-all' surveillance device category, but it would be difficult to formulate a provision that covers yet unknown devices and their uses. Compounding this difficulty is the need to fit this 'catch all' category (and corresponding offence) within the existing SDA framework which is primarily used to regulate law enforcement use of surveillance practices.

6.131 The proposed monitoring and reporting functions of the regulator should help to ensure that the government is regularly informed about new surveillance practices as they develop. This will enable the SDA(Vic) to be amended as the need arises without needing to develop a catch all category. The commission invites submissions on this issue.

Removing the participant monitoring exception

6.132 The prohibitions in the SDA (Vic) concerning the use of listening devices and optical surveillance devices do not extend to a person who uses one of those devices to record a conversation or activity in which they are a participant.[213] This is known as participant monitoring. The SDA (Vic) permits a person who is a party to a conversation or activity to record that conversation or activity without the knowledge or consent of the other people involved.[214] The SDA (Vic) does prohibit a person from knowingly communicating or publishing a record of a private conversation or activity in which that person participated without the consent of the other participants, subject to some exceptions.[215]

6.133 In 1983 the ALRC considered whether participant monitoring involving listening devices should be prohibited. It indicated that it was not desirable to do this,[216] and noted that participant monitoring is an accepted practice in the private sector.[217] The ALRC also suggested that there is no evidence of harmful social effects from participant monitoring.[218] The ALRC also noted that 'in all the States in which legislation exists to regulate the use of listening devices, participant monitoring, in one form or another, is allowed'.[219]

6.134 Support for participant monitoring has since waned. As we explained in Chapter 5, New South Wales, the ACT, Western Australia, Tasmania and South Australia now prohibit this practice. [220] Exceptions to the prohibitions apply. For example, in New South Wales, the prohibition does not apply if recording the conversation 'is reasonably necessary for the protection of the lawful interests of that principal party', or if the recording 'is not made for the purpose of communicating or publishing the conversation, or a report of the conversation, to persons who are not parties to the conversation'.[221] The ACT, Tasmanian and WA legislation have a similar exception.[222] The exception in the South Australia legislation is broader and includes the situation where the use of the listening device is 'in the course of duty of that person, in the public interest or for the protection of the lawful interests of that person'.[223] Like the SDA (Vic), all five states and territories prohibit communicating or publishing a record of a private conversation even when a person has been a party to it.[224]

6.135 While the restriction on communicating or publishing a record of a private conversation in which a person participated goes some way to protecting the expectation of privacy, it may not be sufficient. For example, once a record is made, it remains vulnerable to use and dissemination, if not by the party who recorded it, then by a third party who

199 'Tighter Rules on Camera Phones', *Herald Sun* (Melbourne), 1 July 2004, 1.

200 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info sheet 05.03 (2003) 4.

201 There may be circumstances where police should not have to obtain a warrant to conduct surveillance in toilet areas, shower areas, and change rooms. Section 26 of the SDA (Vic) allows senior officers to authorise surveillance (subject to later approval by a court) where it is impractical to first obtain a warrant. However, emergency authorisation is currently limited to situations where there is an imminent threat of serious violence to a person or of substantial damage to property. It may be desirable to extend the grounds in section 26 to include offences of the type that may occur in toilet areas, shower areas, and change rooms, such as sexual offences against children.

202 Roundtables 2, 8, 9, 10, 12, 13, 14, 15, 20, 21, 24, 25, 26, 27.

203 See, eg, Office of the Privacy Commissioner of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (March 2006). <www.privcom.gc.ca/information/guide/vs_060301_e.asp> at 18 November 2008; Information Commissioner's Office [UK], *CCTV Code of Practice* (2008) <www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf> at 18 November 2008; Information Commissioner's Office [UK].

204 See, eg, Information Commissioner's Office [UK], *CCTV Code of Practice* (Revised edition 2008) 9 <www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf> at 4 March 2009.

205 Victorian Law Reform Commission, *Workplace Privacy*, Final Report (2005) Rec 30.

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

207 *Surveillance Devices Act 2007* (NSW) ss 4(1), 9.

208 *Surveillance Devices Act 1999* (Vic) s 8(1).

209 If the definition of a tracking device changes as proposed for comment, further consideration is needed about whether the *Telecommunications (Interception and Access) Act 1979* (Cth) or the *Telecommunications Act 1997* (Cth) would provide law enforcement officers with an exception that would allow them to track via mobile phones.

210 *Surveillance Devices Act 1999* (Vic) ss 6–9.

211 Ian Gerard, 'Airport Camera will Screen Passengers for Bird Flu', *The Australian*, 22 February 2006, 6.

212 Selma Milovanovic, 'Blown Away by New Technology', *The Age* (Melbourne), 30 December 2005, 4.

213 That approach contrasts with that taken in equivalent legislation in some other Australian jurisdictions. Participant monitoring is discussed in detail in chapter 5.

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

215 *Surveillance Devices Act 1999* (Vic) ss 11(1)–(2).

216 Australian Law Reform Commission, *Privacy* Report No 22 (1983)[1133].

217 Ibid [1129].

218 Ibid [1130].

219 Ibid.

220 *Surveillance Devices Act 2007* (NSW) s 7(1)(b); *Listening Devices Act 1992* (ACT) s 4(1)(b); *Surveillance Devices Act 1998* (WA) s 5(1)(b); *Listening Devices Act 1991* (Tas) s 5(1)(b); and *Listening and Surveillance Devices Act 1972* (SA) s 4.

221 *Surveillance Devices Act 2007* (NSW) s 7(3)(b).

222 *Listening Devices Act 1992* (ACT) s 4(3)(b); *Listening Devices Act 1991* (Tas) s 5(3)(b); *Surveillance Devices Act 1998* (WA) 5(3)(d).

223 *Listening and Surveillance Devices Act 1972* (SA) ss 4, 7(1).

224 *Surveillance Devices Act 2007* (NSW) s 11; *Listening Devices Act 1992* (ACT) s 5; *Listening and Surveillance Devices Act 1972* (SA) s 5; *Surveillance Devices Act 1998* (WA) s 9; *Listening Devices Act 1991* (Tas) s 9.

Options for Reform

is able to gain access to it. Moreover, the exceptions to the prohibition on recording and publishing a record of a conversation or activity that you are a participant in are relatively broad, including whether it is in the public interest or for the protection of a lawful interest.[225]

6.136 Consideration should therefore be given to amending the SDA (Vic) to remove the participant monitoring exception that applies to the use of listening devices. This step would bring the SDA (Vic) in line with legislation in other states. Similar exceptions to those existing in other states would ensure that participant monitoring remains legal in limited and appropriate circumstances.

6.137 The participant monitoring exception to the prohibition on the use of optical surveillance devices also needs reconsideration. For example, it is strongly arguable that it is unacceptable for a person who participates in a consensual sexual act to record that act with an optical surveillance device without the consent of the other person. The surveillance devices legislation in Western Australia recognises this and prohibits the use of an optical surveillance device 'to record visually a private activity to which that person is a party'.[226]

6.138 Amendments to participant monitoring may have implications for some activities of police. Participant monitoring can assist in gathering evidence of criminal activity. The law currently permits a police officer to monitor a conversation or activity to which he or she is not a party with the permission of one party if some other conditions are met.[227] The proposed changes to the SDA (Vic) would require police to apply for a warrant or emergency authorisation to monitor a conversation or activity in these circumstances. Consideration should be given to devising an exception which would permit current law enforcement practices to continue.

Introducing a civil enforcement regime in the SDA (Vic)

6.139 There may be advantages in broadening the way in which the various prohibitions in the SDA (Vic) are enforced. At present, enforcement takes place via the criminal law. The penalties for breaching sections 6, 7 and 8 are severe. The maximum penalty is two years imprisonment and/or 240 penalty units (currently $27,221).[228] A corporation is liable to a maximum penalty of 1,200 penalty units (currently $136,104).[229]

6.140 It may be timely to consider the introduction of civil penalties, either instead of or in addition to criminal penalties in order to deal with less serious breaches of the SDA (Vic). Civil penalties would provide greater flexibility in enforcement. The commission is not aware of any successful prosecutions under the Act since its inception on 1 January 2000. One explanation may be that police and prosecutors regard the sanctions as too severe given the nature of the violations.

6.141 There is growing support for the use of civil penalties when dealing with many violations of the law. Various commentators have suggested that it is important to avoid over-use of the criminal law because:

- to do so may undermine the legitimacy and strength of criminal punishment[230]
- regulators may be reluctant to use the full force of the criminal law[231]
- the stigma of criminal guilt may be attached to behaviour for which it is not warranted.[232]

6.142 In 2007 the Commonwealth Attorney-General's Department stated in *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* that civil penalties are most likely to be appropriate and effective where:

- criminal punishment is not merited (for example, offences involving harm to a person or a serious danger to public safety should always result in a criminal punishment)
- the penalty is sufficient to justify court proceedings
- there is corporate wrongdoing.[233]

6.143 These matters were considered by the ALRC when it recommended a civil penalties regime for breaches of the Privacy Act (Cth).[234] The ALRC concluded that 'criminal sanctions would be disproportionate to the level of harm caused by a serious or repeated interference with an individual's privacy.'[235]

6.144 Other advantages of a civil penalties regime cited by the ALRC are the lower burden of proof (proof on the balance of probabilities as opposed to proof beyond reasonable doubt), and greater procedural flexibility.[236] In addition, the ALRC has noted that reliance on a civil penalties regime, rather than criminal procedures, is likely to reduce the cost and complexity of the regulatory process.[237] This is consistent with the current approach taken by the Victorian government—which 'continues to work towards minimising [the regulatory] burden' on 'businesses, not-for-profit organisations, government sector organisations…and society as a whole'.[238]

6.145 It might be appropriate to retain some criminal penalties in the SDA (Vic) if a civil penalties regime is introduced. A number of existing pieces of legislation include both civil penalties and criminal offences. For example, under the *Trade Practices Act 1974* (Cth) (TPA) a breach of Part IV's restrictive trade practices provisions will result in civil penalties,[239] while criminal sanctions apply for a breach of the Part VC consumer protection provisions.[240] The *Environmental Protection and Biodiversity Conservation Act 1999* (Cth) (EPBCA) also provides for civil and criminal penalties.[241]

6.146 There are many ways in which civil penalties and criminal sanctions could work together in the SDA (Vic). One would be to criminalise repeated or 'serious and wilful' breaches of the Act, leaving other breaches, such as first offences or those involving inappropriate use of a surveillance device for private 'entertainment' purposes, to be dealt with by way of civil penalty. Another option would be to give the regulator responsibility for developing guidelines about when an alleged violation of the Act ought

225 *Surveillance Devices Act 1999* (Vic) s 11(2)(b).

226 *Surveillance Devices Act 1998* (WA) s 6(1)(b).

227 Provided the law enforcement officer is acting in accordance with his or her duty and reasonably believes that it is necessary to monitor or record for the protection of any person's safety. *Surveillance Devices Act 1999* (Vic) 6(2)(c).

228 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1). In the case of the prohibition on law enforcement use of a data surveillance device, a maximum penalty of one year imprisonment and/or 120 penalty units: *Surveillance Devices Act 1999* (Vic) s 9(1). The value of a penalty unit for the 2008–09 financial year is $113.42 and changes yearly to take into account inflation: *Monetary Units Act 2004* (Vic) s 5; Victoria, 'Monetary Units Act 2004: Notice under Section 6 Fixing the Value of a Fee Unit and a Penalty Unit', *Victorian Government Gazette*, Parl Paper No S66 (2008).

229 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1).

230 Mirko Bagaric, 'The "Civil-isation" of the Criminal Law' (2001) 25(4) *Criminal Law Journal* 184, 185.

231 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* Report No 95 (2002) 113 citing Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999) 36; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992) 36.

232 Mirko Bagaric, 'The "Civil-isation" of the Criminal Law' (2001) 25(4) *Criminal Law Journal* 184, 185.

233 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers: Interim new edition — uncleared draft* (2007), [7.2].

234 The ALRC recommended the Privacy Act be amended to 'allow the Federal Privacy Commissioner to seek a civil penalty in the Federal Court or Federal Magistrates Court where there is a serious or repeated interference with the privacy of an individual': Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) Rec 50-2. Currently, the Act empowers the Privacy Commissioner to make orders — including the payment of compensation or that other action be taken (s 52) — but does not impose civil penalties or criminal offences in most circumstances. The Act does contain a number of criminal offences in relation to specific actions, including the disclosure of information (s 80Q); and credit reporting (ss 18K, 18L, 18N, 18P, 18R).

235 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [50.50].

236 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia* Report No 95 (2002) [2.81].

237 Ibid [3.37] citing Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy and Practice* (1999) 38; and Dimity Kingsford-Smith, 'US Corporate Scandals Highlight Importance of Effective Regulation', *The Age* (Melbourne), 19 August 2002, 2.

238 Department of Treasury and Finance, *Victorian Guide to Regulation incorporating: Guidelines made under the 'Subordinate Legislation Act 1994' and Guidelines for the Measurement of Changes in Administrative Burden* (2nd ed, 2007) i.

239 Corporations face civil penalties up to a maximum of the greater of $10 million or 3 times the value of any illegal gain or, if the illegal gain cannot be quantified, 10% of the company's turnover in the preceding twelve months. Individuals face penalties up to a maximum of $500 000. *Trade Practices Act 1974* (Cth) s 76.

240 There are fines of up to $1 100 000 for corporations and $220 000 for individuals. See *Trade Practices Act 1974* (Cth) Part VC and s 6.

241 See, eg, ss 20(1)(a) and 20A(1) of the *Environmental Protection and Biodiversity Conservation Act 1999* (Cth).

to be prosecuted for criminal sanction and when civil penalties enforcement proceedings may be appropriate. The TPA Amendment Bill contains both civil and criminal prohibitions in relation to serious cartel behaviour.[242] The Bill contains a provision which requires the regulator (in this case the ACCC) and the DPP to develop guidelines about the factors that are relevant in determining when the regulator should refer a matter to the DPP for prosecution. Guidelines also play a role in the ARLC's recent proposal that the Federal Privacy Commissioner 'develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty' under the Privacy Act would be made.[243]

6.147 If civil penalties are introduced into the SDA (Vic) there should be a provision which ensures that both civil and criminal proceedings are not instituted against an individual or body corporate for the same conduct. Provisions of this nature have been included in both the TPA and EPBCA.[244]

Clarifying when there is implied consent

6.148 The SDA could be amended to clarify the circumstances in which a person may be taken to have consented to a particular form of surveillance in a public place. The prohibitions concerning the use of surveillance devices in public places do not apply when the surveillance target consents. That consent may be express or implied. The notion of implied consent can be difficult when dealing with common surveillance practices. Does the existence of a sign warning of the use of a surveillance device mean that a person has given implied consent to the monitoring if he or she does not leave the area in question? How should we deal with circumstances where a person objects to the monitoring but has no choice about being in a particular public place?

6.149 The ALRC recommended in its privacy report that the OPC develop guidelines to assist agencies and organisations when deciding how to obtain implied consent for the purposes of the Privacy Act (Cth).[245] The proposed public surveillance regulator could be given a similar function to devise guidelines to assist people how to obtain implied consent for the purposes of the SDA (Vic).

QUESTIONS: CHANGES TO CLARIFY AND STRENGTHEN THE SDA (VIC)

18. Should the SDA (Vic) expressly prohibit the use of an optical surveillance device in toilet areas, shower areas, and change rooms?
19. Should the definition of 'tracking device' in the SDA (Vic) be amended so that it includes all devices capable of determining the geographical location of a person or an object?
20. Should the SDA (Vic) be amended to include a new 'catch-all' category of surveillance devices to cover those devices that do not fit within the Act's existing listening, optical, tracking and data surveillance categories? How could this be done?
21. Should the exemption for participant monitoring in the SDA (Vic) be removed? If so, should this also be done for both listening and optical surveillance devices?
22. Should the enforcement regime of the SDA(Vic) be extended to include civil penalties?
23. Should the regulator's proposed powers to develop guidelines be extended to clarifying the meaning of consent in the SDA (Vic)? If so how should the meaning of consent be clarified?

OPTION 6—CREATING A STATUTORY CAUSE OF ACTION FOR SERIOUS INVASIONS OF PRIVACY

6.150 Like their counterparts in the United Kingdom and New Zealand, Australian courts appear to be moving towards recognising a common law cause of action for invasion of privacy. It is difficult to predict how long this process will take because it depends upon an appropriate case making its way to the High Court of Australia. The costs risks for any individual who seeks to litigate this issue in the High Court are great. An alternative approach, used in some parts of Canada and the United States,[246] and which has been

recommended by the ALRC,[247] is to create a statutory cause of action for serious invasion of privacy.

6.151 It is timely to consider whether Victorian legislation should contain a cause of action for serious invasion of privacy. Given the amount of work undertaken by the ALRC in relation to this issue, it makes sense to consider the detail of its proposal. The ALRC suggested that the relevant legislation could contain a non-exhaustive list of the types of serious invasion of privacy that fall within the cause of action. They include where:

- there has been an interference with an individual's home or family life
- an individual has been subjected to unauthorised surveillance
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed
- sensitive facts relating to an individual's private life have been disclosed.[248]

The ALRC did not define or expand upon the meaning of 'unauthorised surveillance'. In Canadian provincial privacy legislation[249] violations of privacy, which include unauthorised surveillance, give rise to a cause of action when undertaken 'without claim of right' which has been interpreted to mean without 'legal justification or excuse'.[250] An example of surveillance deemed to be without legal justification or excuse was the filming by an insurance investigator of the daughter of a disability insurance claimant through the window of the claimant's home while she was changing her clothing.[251]

6.152 Unlike the general law action for breach of confidence in the UK and the tort of privacy in New Zealand, the ALRC's proposed statutory cause of action is not limited to disclosure of private information. Mere interference with privacy, without publication of private facts, may constitute an invasion of privacy provided other elements of the cause of action are made out.

6.153 The ALRC reported that it received strong support for the creation of a statutory cause of action for serious invasions of privacy, including from the Federal Privacy Commissioner.[252] Some of those opposing creation of the cause of action suggested that the *Privacy Act* (Cth) provides sufficient protections,[253] and expressed concern about the possibility of privileging privacy over other rights, such as freedom of expression.[254] Media organisations, professional and amateur street artists, and others expressed concern about their ability 'to watch, film, record and gather information without any further restrictions'.[255]

6.154 A Victorian statutory cause of action may operate as a useful adjunct to the other regulatory options we have proposed by providing a remedy for serious invasions of privacy by the inappropriate use of surveillance in public places. Any statutory cause of action is unlikely to cause a marked increase in litigation because the costs rules associated with civil proceedings provide a strong disincentive against frivolous and speculative claims.

Elements of the proposed cause of action

6.155 The ALRC recommended that the essential elements of the statutory cause of action should be:

- that the plaintiff had a reasonable expectation of privacy in the circumstances
- that the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.[256]

These elements reflect comments made by Chief Justice Gleeson in *Lenah*,[257] which were drawn from the US privacy tort often referred to as public disclosure of private facts. This tort is discussed in Chapter 5.[258]

242 Trade Practices Amendment (Cartel Conduct and Other Measures) Bill 2008 (Cth).

243 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 2: Final Report* 108 (2008) Rec 50-3.

244 *Trade Practices Act 1974* (Cth) s 76B; *Environmental Protection and Biodiversity Conservation Act 1999* (Cth) ss 486A, 486B, 486C, 486D.

245 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [19.30], [19.68], Rec 19-1.

246 See Fred H Cate, *Privacy in the Information Age* (1997) 88; John D R Craig, 'Invasion of Privacy and Charter Values: The Common-Law Tort Awakens' (1997) 42 *McGill Law Journal* 355.

247 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) ch 74, in particular [74.181]–[74.191]. See also the recommendations of the New South Wales Law Reform Commission in New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007) ch 7.

248 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) Rec 74-1

249 *Privacy Act*, RSBC 1996, c 373, s 1(1); *Privacy Act*, RSS 1978, c P-24, s 2–3; *Privacy Act*, RSNL 1990, c P-22, s 3(1), 4(a).

250 *Hollinsworth v BCTV* (1998) 59 BCLR (3d) 121 (British Columbia Court of Appeal).

251 *Milner v. Manufacturers Life Insurance Company* [2005] BCSC 1661, cited in British Columbia Law Institute, *Report on the Privacy Act of British Columbia* BCLI Report No 49 (2008) 9.

252 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [74.85].

253 Ibid [74.88].

254 Ibid [74.91].

255 Ibid [74.95]–[74.96].

256 Ibid Rec 74-2.

257 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

258 That test is also the one adopted by the New Zealand courts: see, eg, *Hosking v Runting* [2004] NZCA 34.

Chapter 6 Options for Reform

A reasonable expectation of privacy

6.156 The first requirement—a reasonable expectation of privacy—is common to most privacy-based actions, and has been described as being at the 'core' of a tort of privacy intrusion.[259] It is an objective test because the plaintiff's expectation of privacy must be reasonable in the circumstances and consistent with community standards.[260]

6.157 Presence in a public place does not preclude the requirement of a reasonable expectation of privacy. The ALRC notes:

> *circumstances giving rise to the cause of action should not be limited to activities taking place in the home or in private places…The appropriate test is whether the circumstances give rise to a reasonable expectation of privacy, regardless of whether the activity is in public or private.*[261]

6.158 In a number of common law countries, a cause of action for invasion of privacy is available to people who suffered harm because of public place surveillance activities. We discuss these developments as well as those in the common law in Chapter 5.

Act or conduct complained of is highly offensive

6.159 A further element of the proposed cause of action is that the conduct complained of would be highly offensive to a reasonable person of ordinary sensibilities. This element derives from the disclosure of private facts tort in the US and New Zealand.[262] Chief Justice Gleeson referred to this element in *Lenah* and noted its utility:

> *There is no bright line which can be drawn between what is private and what is not…The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.*[263]

6.160 The requirement that conduct complained of be highly offensive also helps limit the cause of action to 'egregious circumstances'[264] and ensures that the important countervailing interest of 'freedom of expression is respected and not unduly curtailed in the great run of circumstances'.[265] The requirement also helps ensure that the law does not protect 'unduly sensitive' plaintiffs. A plaintiff will succeed only 'where the defendant's conduct is thoroughly inappropriate and the complainant suffered serious harm as a result'.[266] The ALRC provided examples of some matters that would be actionable:

- someone sending a DVD of himself and his girlfriend engaged in sexual activity to the girlfriend's neighbours and employers
- setting up a hidden camera in a toilet and posting images to a website.[267]

6.161 What sort of conduct would be highly offensive to a reasonable person of ordinary sensibilities? The case law in other countries is instructive. In *Andrews v TVNZ*,[268] for example, the New Zealand High Court held that broadcast of footage and conversation between an injured couple in the course of rescue after their motor vehicle accident was not highly offensive to a reasonable person of ordinary sensibilities.[269]

6.162 The requirement that the conduct complained of be highly offensive features less strongly in the extended action for breach of confidence developed by the UK courts.[270] In *Campbell v MGN Ltd*,[271] Lord Hope stated that the 'highly offensive test' only applies in cases where there is room for doubt about whether information disclosed was private; it is not to be used where information can easily be identified as private:[272]

> *If the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected. So there is normally no need to go on and ask whether it would be highly offensive for it to be published.*[273]

6.163 This view was shared by the UK Court of Appeal in *Murray v Big Pictures (UK) Ltd*,[274] where the Court said that the 'highly offensive test' is not used for determining whether privacy has been breached, but whether the breach of privacy is not outweighed by countervailing considerations such as freedom of expression.[275] *Murray v Big Pictures (UK) Ltd* concerned

a photograph taken covertly on a public street of famous author J.K. Rowling and her family. The Court distinguished the UK expanded breach of confidence test from the invasion of privacy tort in New Zealand where the 'highly offensive test' is an essential element of the cause of action.[276]

No countervailing public interests

6.164 A further element of the proposed cause of action developed by the ALRC is whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest.[277] Other matters of public interest may include being informed about matters of public concern and freedom of expression.[278]

6.165 This balancing approach is also consistent with the Charter's approach to human rights in which the rights are not absolute.[279] According to the ALRC, incorporating a balancing test within the cause of action itself, rather than as a defence, recognises the importance of freedom of expression. If freedom of expression was merely a defence, unmeritorious claims could proceed with defendants having to wait until the defence case to raise their public interest defence.[280]

Other aspects of the cause of action

6.166 Another important consideration is the state of mind required of the defendant in order to establish liability. The ALRC's recommended cause of action requires conduct which is deliberate or reckless, and not simply negligent. The inclusion of an element of wilfulness is consistent with the Canadian statutory privacy torts,[281] although it is at odds with information privacy laws. The inclusion of recklessness addresses the fact that 'indifference to the consequences of an invasion of privacy is as culpable as intentionally invading another's privacy'.[282] Exclusion of negligent acts conforms with the view that 'including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far'.[283]

6.167 The ALRC's proposed cause of action does not require any proof of actual damage, thereby extending its reach to conduct that causes insult or humiliation, rather than physical or economic harm. The ALRC suggested that a successful plaintiff should have access to a wide range of remedies including ordinary and aggravated damages (but not exemplary damages), an account of profits, an injunction, an order requiring the respondent to apologise to the claimant, a correction order, an order for the delivery up and destruction of material, and a declaration. The ALRC did not recommend any limits to the amount of damages that could be awarded. With the exception of the recent *Mosely*[284] case, damages awarded by courts for surveillance-related activities have been very modest.[285]

259 Hong Kong Law Reform Commission, *Civil Liability for Invasion of Privacy*, Report (2004) [6.26].

260 Peter Nygh and Peter Butt (eds), *Butterworths Australian Legal Dictionary* (1997) 984, 'Reasonable Person'.

261 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [74.124].

262 See *Restatement (Second) of Torts* (1977) s 652A–652E; *Hosking v Runting* [2004] NZCA 34.

263 *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199, [42].

264 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008)127.

265 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [74.135].

266 Ibid [74.135].

267 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) 128.

268 [2006] NZHC 1586.

269 In determining whether the plaintiffs could establish liability for invasion of privacy, the New Zealand High Court followed the decision in *Hosking v Runting* [2003] 3 NZLR 285.

270 For example, it has been suggested by the House of Lords in *Campbell v MGN* [2004] 2 AC 457 that it is unnecessary where the information is clearly private in nature: [96] (Lord Hope), and that an objective test based on reasonable expectation of privacy is much clearer: [21] (Lord Nicholls).

271 [2004] 2 AC 457.

272 *Campbell v MGN Ltd* [2004] 2 AC 457, [94].

273 *Campbell v MGN Ltd* [2004] 2 AC 457, [96].

274 [2008] EWCA Civ 446.

275 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, [26].

276 *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446, [48]–[49].

277 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) Rec 74-2.

278 Ibid.

279 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 7. Human Rights Unit, Department of Justice, *Human Rights and Responsibilities: Draft Charter Guidelines*, 40, [2.2].

280 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) [74.144], [74.147].

281 *Privacy Act*, RSBC 1996, c 373, s 1(1); *Privacy Act*, RSS 1978, c P-24, s 2; *Privacy Act*, RSNL 1990, c P-22, s 3(1).

282 Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* Report (2004) [6.71].

283 NSW Law Reform Commission, *Invasion of Privacy* Consultation Paper 1 (2007) [7.24].

284 *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777. Mosley was awarded £60,000 for the publication of photographs and videos of sexual activities conducted at his apartment:

285 For example, the model Naomi Campbell was awarded only £3500 for the publication of the articles and photographs relating to her attendance at Narcotics Anonymous meetings: *Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB), [165]

Chapter 6 Options for Reform

6.168 The ALRC recommended that there be three defences to the proposed statutory cause of action for serious invasion of privacy:

- where the act or conduct is incidental to the exercise of a lawful right of defence of person or property
- where the act or conduct is required or authorised by or under law
- where publication of the information is subject to privilege under the law of defamation.[286]

6.169 In addition to these defences, one option worthy of consideration is whether compliance with a mandatory code of practice (as discussed in Option 3) should constitute an additional defence to the proposed cause of action. While not directly canvassed by the ALRC, this proposal probably falls within one of its proposed defences—namely that the conduct in question was authorised by law.[287]

6.170 The ALRC recommended that the Federal Privacy Commissioner provide information to the public about any new statutory cause of action. A similar role could be performed by the proposed regulator if a statutory cause of action for serious invasion of privacy is introduced in Victoria.

QUESTIONS: CREATING A STATUTORY CAUSE OF ACTION FOR SERIOUS INVASIONS OF PRIVACY

24. Should there be a statutory cause of action for serious invasions of privacy along the lines proposed by the ALRC?

SUMMARY OF QUESTIONS TO GUIDE SUBMISSIONS

PRINCIPLES TO GUIDE PUBLIC PLACE SURVEILLANCE

1. Do you agree with the draft principles proposed by the commission to guide policy making about public place surveillance?
2. Should the once-off or intermittent use of surveillance practices by individuals be regulated?

A NEW ROLE FOR AN INDEPENDENT REGULATOR

3. Do you agree with the proposal that an independent regulator should have responsibility for monitoring the use of public place surveillance in Victoria? Who should perform this role?

SPECIFIC FUNCTIONS OF THE REGULATOR

4. Should the regulator be given the functions proposed by the commission?
5. Are there any other functions that should be given to the regulator?
6. Would a registration scheme assist the regulator to acquire information about surveillance use? Is such a scheme practical? Should some users be exempt from registration requirements?
7. What (if any) investigatory powers should be given to the regulator?
8. Should the regulator have an own motion investigatory power in order to identify systemic problems with surveillance in public places?
9. Should the regulator have the power to develop advisory guidelines which explain the law concerning surveillance in public places?

VOLUNTARY BEST-PRACTICE STANDARDS

10. Would voluntary best-practice standards developed or approved by the regulator be useful?
11. Is linking voluntary best-practice standards to government procurement criteria a good strategy for encouraging responsible use of surveillance practices? Are there other strategies for encouraging compliance with the voluntary standards?

MANDATORY CODES OF PRACTICE

12. Should there be mandatory codes, if so, what conduct should they regulate?
13. If mandatory codes are introduced, should the regulator have the power to approve industry codes that operate in their place?
14. Should the regulator be empowered to investigate complaints made about potential breaches of a mandatory code? How broad should any such powers be?
15. What kind of sanctions should be imposed for breaches of a mandatory code?

A LICENSING SYSTEM FOR SOME SURVEILLANCE PRACTICES

16. Should users of some forms of surveillance practices be required to obtain a license from a regulator?
17. Are there any surveillance practices in Victorian public places that are particularly concerning? If so why?

CHANGES TO CLARIFY AND STRENGTHEN THE SDA (VIC)

18. Should the SDA (Vic) expressly prohibit the use of an optical surveillance device in toilet areas, shower areas, and change rooms?
19. Should the definition of 'tracking device' in the SDA (Vic) be amended so that it includes all devices capable of determining the geographical location of a person or an object?

286 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice, Volume 3, Final Report* 108 (2008) [74.169]. As noted above at 6.164, a public interest justification for the invasion of privacy is not a defence to the cause of action, because it is to be considered by the court at an earlier stage, in deciding whether the cause of action is made out.

287 Ibid. The ALRC also noted: 'The ALRC's view is that the definition of 'law' for the purposes of the 'required or authorised by or under law' exception should include Commonwealth and state and territory Acts and delegated legislation as well as duties of confidentiality under common law or equity': Ibid [74.172]. This approach is also consistent with the approach taken under NSW anti discrimination laws, which allow for the development of codes of practice, and provide that evidence of compliance with a code may be considered by the Administrative Decisions Tribunal: *Anti-Discrimination Act 1977* (NSW) s 120A.

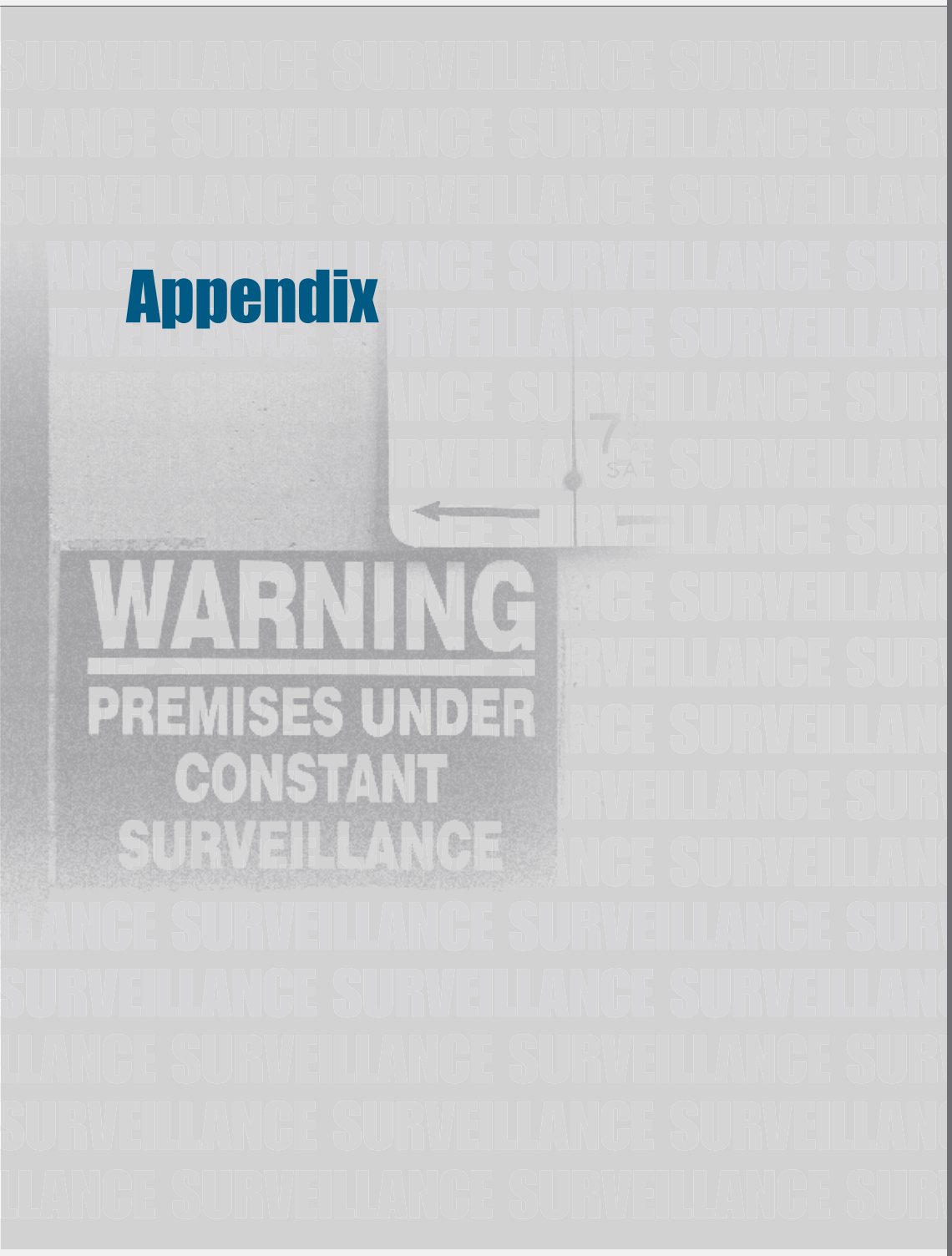
Chapter 6 Options for Reform

20. Should the SDA (Vic) be amended to include a new 'catch-all' category of surveillance devices to cover those devices that do not fit within the Act's existing listening, optical, tracking and data surveillance categories? How could this be done?
21. Should the exemption for participant monitoring in the SDA (Vic) be removed? If so, should this also be done for both listening and optical surveillance devices?
22. Should the enforcement regime of the SDA(Vic) be extended to include civil penalties?
23. Should the regulator's proposed powers to develop guidelines be extended to clarifying the meaning of consent in the SDA (Vic)? If so how should the meaning of consent be clarified?

CREATING A STATUTORY CAUSE OF ACTION FOR SERIOUS INVASIONS OF PRIVACY

24. Should there be a statutory cause of action for serious invasions of privacy along the lines proposed by the ALRC?

Appendix



Consultations and Submissions

CONSULTATION PARTICIPANTS

ABC News
ADT Australia
ANZ Bank
Australian Commercial and Media Photographers
Australian Communications and Media Authority
Australian Photographic Society
Australian Press Council
Australian Privacy Foundation
Australian Retailers Association
Australian Security Industry Association
Australian Subscription Television and Radio Association
Box Hill Institute of TAFE
Bus Association of Victoria
Business Victoria (Small Business Victoria)
Centre Safe Committee Lilydale
Centro Properties Group
Channel Ten News
City of Ballarat
City of Greater Dandenong
City of Greater Geelong Council
City of Port Phillip
CityLink
Clubs Victoria
Coles Group
Colonial First State Property Management
Commercial Radio Australia
Communications Law Centre
Connex
Consumer Affairs Victoria
Corrs Chambers Westgarth
Crimestoppers
Crown Casino
Darebin City Council
Deakin University
Electronic Frontiers Australia
Federation Square
Film Victoria
Fitness Victoria
Greyhound Racing Victoria

Herald and Weekly Times
Holding Redlich
Holmesglen Institute of TAFE
Human Rights Law Resource Centre
Inner Range
Institute of Body Corporate Managers
Institute of Mercantile Agents
Islamic Council of Victoria
Kangan Batman Institute of TAFE
LaTrobe City Council
Leader Newspapers
Liberty Victoria
Marriner Theatres
Maurice J Kerrigan and Associates
Melbourne City Council
Melbourne Cricket Ground Trust
Melbourne Exhibition and Convention Centre
Mental Health Legal Centre
Minter Ellison
Monash University
Municipal Association of Victoria
Museum Victoria
Myer
National Gallery of Victoria
National Intelligent Transport Systems Centre
Neighbourhood Watch
Parks Victoria
Pharmacy Guild of Australia
Port of Melbourne Corporation
Privacy Victoria
Property Council of Australia
Public Interest Law Clearing House (Homeless Persons' Legal Clinic)
Queen Victoria Market
Racing Victoria Limited
RACV
Regional Aboriginal Justice Advisory Committees (Chief Executive Officers)
RMIT University
Shopping Centre Council of Australia
Siemens Limited
SMI Security Group
Southeast Water

Consultations and Submissions

Southern Cross Station

Southern Health

State Library of Victoria

State Sport Centres Trust

Stonnington City Council

Swinburne University

Telstra Dome

Tourism Victoria

Transport Accident Commission

University of Ballarat

University of Melbourne

V/Line

VicRoads

Victoria Police

Victoria University of Technology

Victorian Arts Centre Trust

Victorian Authorised Newsagents Association

Victorian Automobile Chamber of Commerce

Victorian College of the Arts School of Film and Television (University of Melbourne)

Victorian Commission for Gambling Regulation

Victorian Council of Social Service

Victorian Department of Education and Training (now the Department of Education and Early Childhood Development)

Victorian Department of Human Services (Office of Housing)

Victorian Department of Infrastructure including Victorian Taxi and Tow-Truck Directorate

Victorian Department of Innovation, Industry and Regional Development including Small Business Victoria (formerly the Office of Small Business)

Victorian Department of Justice [Victoria] (Civil Law Policy, Justice Policy, Crime and Violence Prevention, Court Services, Court Security, Indigenous Issues Unit, Melbourne Magistrates' Court, Office of Gaming and Racing, Liquor Licensing)

Victorian Department of Planning and Community Development (Office for Youth)

Victorian Department of Sustainability and Environment

Victorian Detective Services

Victorian Security Industry Advisory Committee

Victorian Workcover Authority

Welfare Rights Unit

Woolworths

Yarra Trams

Yarra Valley Water

Youth Affairs Council of Victoria

Youthlaw

INDIVIDUALS

Roger Clarke, Consultant, eBusiness information infrastructure, data surveillance and information privacy

Mike Thompson, Director and CEO, Linus Information Security Solutions

David Watts, Victorian Commissioner for Law Enforcement Data Security

Dr Deane Wilson, Senior Lecturer, Criminology, School of Political and Social Inquiry, Monash University

SUBMISSIONS

1.Confidential

2. Kyle McDonald

3. Troy Ellis

4. Anonymous

5. Karen Young

Recent commission publications

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 Position Paper One: Access (May 2005)

Assisted Reproductive Technology Position Paper Two: Parentage (July 2005)

Family Violence Police Holding Powers: Interim Report (September 2005)

Workplace Privacy: Final Report (October 2005)

Review of the Bail Act: Consultation Paper (November 2005)

Have Your Say About Bail Law (November 2005)

Assisted Reproductive Technology Position Paper Three: Surrogacy (November 2005)

Implementing the Uniform Evidence Act: Report (February 2006)

Uniform Evidence Law: Final Report (February 2006)

Review of Family Violence Laws: Report (March 2006)

Review of Family Violence Laws: Final Report Summary (March 2006)

Residential Tenancy Databases: Report (April 2006)

Civil Justice Review Consultation Paper (September 2006)

Assisted Reproductive Technology & Adoption: Final Report (June 2007)

Review of the Bail Act: Final Report (October 2007)

Civil Justice Review: Report (May 2008)

Law of Abortion: Final Report (May 2008)

Assistance Animals: Consultation Paper (July 2008)

Jury Directions: Consultation Paper (September 2008)

Assistance Animals: Final Report (January 2009)

Victorian
Law Reform
Commission

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

Level 3, 333 Queen St
Melbourne Victoria 3000 Australia

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

Printed on 100% recycled paper